EVALUA

INTRODUCCIÓN

La Agencia Española de Protección de Datos[1] tiene como una de sus tareas prioritarias proporcionar guías, recomendaciones y elementos dirigidos tanto a las unidades de la administración responsables del tratamiento de datos de carácter personal como a aquellas otras, como las unidades de informática, que realizan labores de encargados de tratamiento de datos de carácter personal.

Esta tarea se hace más necesaria cuando se trata de responsables de ficheros que almacenan datos de carácter personal que no cuentan inicialmente con los conocimientos o los medios necesarios para conocer su grado de adaptación a la normativa de protección de datos.

Así, y a lo largo de los últimos años la Agencia ha elaborado:

- La *Guía del Responsable de ficheros*, que contiene indicaciones sobre los principios básicos que deben ser tenidos en cuenta para cumplir adecuadamente con la legislación sobre protección de datos
- La *Guía de Seguridad de Datos*, que ayuda a implementar, revisar y aplicar las medidas de seguridad contenidas en el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal.
- La *Guía de Videovigilancia*, que describe todas las cuestiones relacionadas con el tratamiento de imágenes y en particular las relativas a la seguridad y al uso con fines de control laboral.
- La *Guía de protección de datos en las relaciones laborales*, se plantea como objetivo considerar un conjunto de aspectos prácticos a los que las empresas deben enfrentarse habitualmente.

Así mismo, desde el año 2006 se encuentra disponible a través de la página Web de la Agencia el *sistema de NOtificaciones Telemáticas a la AEPD (NOTA)*, que permite a los responsables de ficheros con datos de carácter personal de titularidad pública cumplir con la obligación que la LOPD[2] establece de notificar sus ficheros a la Agencia Española de Protección de Datos a través de una herramienta que le informa y asesora acerca de los requerimientos de la notificación, una vez la administración responsable ha procedido a la publicación de la disposición sobre el fichero correspondiente; de igual forma la notificación mediante formato XML o la recepción de notificaciones a través de la

[1] La Agencia Española de Protección de Datos (AEPD): organismo responsable de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos

[2] LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Dirección Electrónica Única han colaborado en facilitar el proceso de notificación de ficheros.

Por lo tanto, y con el objeto de facilitar tanto a las unidades de la administración pública responsables de ficheros[3] de datos de carácter personal, como a las que realizan labores de encargados de tratamiento[4] sobre datos de carácter personal, la adopción de las obligaciones derivadas de la LOPD y de su Reglamento de desarrollo[5], la AEPD ha puesto a su disposición una herramienta de autoevaluación para comprobar el cumplimiento de la LOPD e igualmente evaluar el cumplimiento de las medidas de seguridad[6] establecidas en el RLOPD.

OBJETO

Esta herramienta de autoevaluación *pretende promover una cultura LOPD* en las administraciones públicas españolas, así como facilitar a los responsables que tratan datos de carácter personal y a los encargados de tratamiento la adopción de las obligaciones derivadas de la LOPD y de su Reglamento de desarrollo.

Creada con la intención de *Comprometer* al responsable de datos de carácter personal con la protección de datos, este test le *permitirá evaluar el grado de cumplimiento de la normativa sobre protección de datos*, permite el autodiagnóstico dentro de cada institución y colaborar en la difusión e integración de los conocimientos en esta materia dentro de la misma.

EVALUA tiene *dos niveles* de autoevaluación: el que corresponde a la *revisión del cumplimiento normativo en materia de protección de datos de carácter personal* y el que corresponde a la *revisión de todas las cuestiones asociadas a las medidas para asegurar la seguridad sobre los datos de carácter personal sobre los que la administración actúa*.

La herramienta de autoevaluación disponible en la Web de la Agencia Española de Protección de Datos (www.agpd.es) será útil a dos perfiles de usuario: por un lado *el responsable del fichero que verificará el cumplimiento de la LOPD* en su organización y por otro lado al *responsable de seguridad que verificará el cumplimiento de las medidas*

---

[3] Responsable de fichero: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

[4] Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

[5] Reglamento de desarrollo de la LOPD (RLOPD): 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.

[6] Seguridad de los datos: las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural; ver apartado *En que consiste, conceptos previos.*

técnicas y organizativas asociadas en lo que respecta a preservar la seguridad de los datos de carácter personal.

EVALUA, procedimiento de diagnóstico basado en un autotest basado en preguntas con respuesta múltiple *facilita un informe* con indicaciones sobre las deficiencias detectadas y recursos que orientan para cumplir con lo dispuesto en la LOPD en los dos ámbitos (cumplimiento y seguridad) descritos y poder adoptar las medidas correctoras correspondientes.

EN QUE CONSISTE, CONCEPTOS PREVIOS

La herramienta EVALUA, sistema sencillo de test que pregunta por las cuestiones en relación con los datos recabados, forma, fines y procedimientos empleados, está dotada de un sistema de autoayuda que pretende poner en contexto toda la información que el usuario demande cuando la está utilizando; así, y desde el comienzo, el navegante se encuentra con la descripción de los elementos que forman parte del producto a su disposición además de todas las definiciones de los conceptos más habituales en lo que respecta a protección de datos de carácter personal.

EVALUA está organizado en base a una encuesta sucesiva, cuyo carácter anónimo contribuirá a asegurar que la realización del Test refleje la situación real de la organización. Además está preparada para poder dejar la tarea de forma temporal si no se dispone del tiempo suficiente, o ha de completarse el conocimiento sobre el fichero que se está trabajando; la herramienta permite retomar el estudio de cualquiera de las dos fases facilitando al usuario un código que será reintroducido en el sistema de forma posterior continuando el test en el punto que se hubiera abandonado.

El Test de Autoevaluación puede ser realizado por el propio responsable del fichero aunque también puede ser realizado por un equipo designado por el responsable o requerir asesoramiento de expertos. En cualquier caso, es recomendable que las personas que se encuentren directamente *relacionadas con el tratamiento de datos* se encuentren involucradas en la realización del Test de Autoevaluación.

Al planificar la realización del Test de Autoevaluación puede ser necesario establecer el *ámbito* que se pretende evaluar, por ejemplo, si existen diversos ficheros o tratamientos, diversos departamentos involucrados, etc. En estos casos, puede ser recomendable planificar la evaluación de cada uno de los ficheros, sistemas de información o tratamientos dependiendo de su homogeneidad.

Como se ha comentado, la primera parte de la herramienta EVALUA, corresponde al TEST de cumplimiento de LOPD, que repasa en seis etapas diferentes el estado en que se encuentre el sistema analizado con respecto a la protección de datos.

Para ellos se ha tomado como base fundamental los contenidos incluidos en la *Guía del Responsable de ficheros*.

Además, la herramienta permite obtener un informe con las deficiencias detectadas para, en su caso, adoptar las medidas correctoras correspondientes.

El usuario que emplea EVALUA, en lo que respecta al TEST de cumplimiento de la LOPD, se encuentra con cuestiones que de forma secuencial pretenden guiarle en su chequeo del estado de cumplimiento de la Ley, en el ámbito que se haya definido para su estudio (un fichero, un grupo de ficheros de una subdirección general o dirección general,..); así:

La primera de las etapas pregunta al usuario, cuando se habla de ficheros de los que son responsables las administraciones públicas, por el *Registro de ficheros*, primera obligación que consiste en proceder a notificar a la AEPD, por el órgano competente de la Administración responsable, el fichero para su inscripción en el Registro General de Protección de Datos (RGPD).

La segunda de las etapas centra las cuestiones sobre la *Información* suministrada en el momento de la recogida de los datos y el *Consentimiento* otorgado en su recogida. Conocer el origen de los datos que la administración trata es fundamental para recomendarle como cumplir con algunas de las obligaciones previstas por la LOPD, la primera de ellas es el *deber de informar* en la recogida de los datos. Cuando se captan datos de una persona existe la obligación de informar de los aspectos básicos del tratamiento que se va a realizar antes de proceder al mismo, esto es, se debe informar que se va a realizar un tratamiento de datos de carácter personal y/o proceder a la incorporación de estos a un fichero, para que fin se recogen los datos, si estos fueran a cederse a terceros, qué administración es responsable del tratamiento y su dirección y donde y ante quien ejercitar los derechos de acceso, rectificación, cancelación y oposición.

De igual forma, para tratar datos hay que tener lo que se denomina *legitimación*, es decir, debe existir alguna razón que justifique que se puedan tratar unos datos concretos. Una forma de legitimación muy habitual es que la persona a la que pertenecen los datos haya manifestado su *consentimiento* de algún modo. No será preciso el consentimiento cuando los datos de carácter personal se *recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias*, este supuesto únicamente afecta al que siendo Administración ejerce funciones públicas. Es esencial que se distinga entre el ejercicio de funciones públicas y la prestación de cualquier tipo de servicio, o el desarrollo de cualquier actividad que no posea esta naturaleza. Cuando un ayuntamiento ejerce sus competencias tributarias, realiza comprobaciones en el padrón municipal, o desarrolla funciones de policía administrativa podrá tratar datos sin consentimiento. Pero si desarrolla actividades que no están en ese marco como por ejemplo abrir un espacio de participación voluntaria en Internet o facilitar una cuenta de correo electrónico a sus ciudadanos para tratar datos necesitará el consentimiento.

Como se ha dicho se podrán tratar datos sin el consentimiento del interesado cuando exista una Ley que obligue a que faciliten estos datos. Por ejemplo, los servicios de sanidad y epidemiología pueden exigir, con fundamento en la LOPD, el acceso a todos los datos de personas que hayan padecido una enfermedad de declaración obligatoria, porque la Ley les habilita para ello[7]. De igual forma la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas obliga a quienes satisfacen rentas del trabajo a practicar retenciones y esta obligación no requiere del consentimiento del trabajador.

Las administraciones públicas tratan en muchas ocasiones datos referidos a infracciones penales o administrativas y estos tratamientos se encuentran entre sus competencias; así mismo debe tener en cuenta que cuando recabe datos especialmente protegidos (ideología, afiliación sindical, religión o creencias, origen racial, salud o vida sexual) los procedimientos de obtención del consentimiento sigue reglas específicas (a no ser que una ley habilite su recogida y tratamiento, como el caso ya descrito de la salud).

La tercera de las etapas del Test de cumplimiento LOPD pregunta, bajo el epígrafe de *Principios* en primer lugar sobre la Calidad de los Datos, recordando que los datos de carácter personal sólo se podrán recoger y someter a tratamiento cuando sean *adecuados, pertinentes y no excesivos* en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Que los datos no sean excesivos significa que se recogerán de modo proporcional, esto es, únicamente los que se necesiten para el tratamiento.

Continúa el principio de calidad especificando que los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Además, serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento sea incorrecto o excesivo, en particular, cuando tales datos resulten inexactos o incompletos, siempre que se tenga conocimiento de que dichos datos no están actualizados.

Por último, este principio de calidad especifica que una vez cesa la finalidad para la que fueron recabados, la legislación precisa que hay que proceder a la cancelación. La cancelación dará lugar, al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. Se entiende por bloqueo de datos la identificación y reserva de datos con el fin de impedir su tratamiento. Mientras los datos están bloqueados es como si estuvieran cancelados a todos los efectos.

[7] Artículo 7. 6 de la LOPD en relación con los datos especialmente protegidos.

De igual forma el *deber de secreto*[8] es un principio en el que la legislación ordena que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estén obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el responsable del fichero.

La cuarta de las etapas del Test de cumplimiento LOPD trata sobre los derechos que la LOPD otorga a las personas cuyos datos trata, el derecho a la protección de datos persigue un objetivo muy preciso: que todos podamos controlar nuestros datos. Para ello se regulan los llamados derechos A.R.C.O[9]: *Derecho de acceso* (facilita que en cualquier momento se pueda saber qué datos se están tratando), *Derecho de rectificación* (permite que se solicite que se rectifiquen los datos erróneos o equivocados), *Derecho de cancelación* (permite que se cese de tratar datos y que se cancelen cuando se solicita y justifica) y *Derecho de oposición* (evita que se traten los datos sin consentimiento o que se cedan a terceros).

Son derechos personalísimos, es decir, que los puede ejercitar únicamente su titular, salvo incapacidad o minoría de edad; así, el afectado o interesado cuyos datos se tratan puede dirigirse un organismos públicos, de los que sabe o presume que tienen sus datos, solicitando información sobre qué datos tienen y cómo los han obtenido, la rectificación de los mismos, la cancelación de los datos en sus ficheros o la oposición a que traten sus datos para un uso o fin determinado. Además son independientes, lo que significa que no hace falta ejercer uno de ellos, por ejemplo el de acceso, para poder ejercer otro, por ejemplo el de cancelación.

Como responsable de ficheros la administración debe contestar en el plazo correspondiente ante el ejercicio de un derecho A.R.C.O. conociendo además que en ciertas circunstancias puede denegarse el ejercicio de los citados derechos.

La quinta de las etapas refiere, bajo el epígrafe de Relación con terceros, conceptos como los de comunicación de datos, acceso a datos, artículo 12 de la LOPD, transferencia internacional de datos, nivel adecuado de protección.

Así, se denomina *comunicación de datos*[10] a toda revelación de datos que se hace a un tercero distinto de la persona cuyos datos se tratan y de la propia organización; el acceso a los datos por una unidad distinta de la misma organización *no* es una comunicación de datos. Para que exista cesión debe tratarse de un tercero, de una persona física o jurídica diferenciada, es importante saber que para que *exista comunicación o cesión de datos*

---

[8] Artículo 10 de la LOPD recoge el Deber de secreto.

[9] El Título III de la LOPD recoge los Derechos de las personas; igualmente el Título VIII del RLOPD los desarrolla.

[10] Artículo 11. 1 de la LOPD: Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

no hace falta la posesión física del dato. Basta con la simple *consulta o con la revelación verbal* del dato. Las comunicaciones de datos son un tratamiento de datos personales que se rige por los principios generales del consentimiento. Por tanto y como regla general *para poder ceder los datos es necesario el consentimiento de la persona cuyos datos se tratan*, o bien *existe una Ley que permita la cesión*. A modo de ejemplo, ante el requerimiento de un juez, la propia LOPD exige que se realice la cesión. El artículo 11.2[11] LOPD recoge supuestos específicos: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público

En multitud de ocasiones se recurre a terceros para que presten servicios que conllevan que se traten datos personales, por ejemplo, cuestiones como la externalización del alojamiento de los sistemas o el mantenimiento de hardware, y sobre todo de software, en muchas ocasiones exige *el acceso a datos de carácter personal*. En estos casos hay un prestador externo de un servicio que accede a datos de los sistemas de información, esta *prestación de servicios* no basta regularla en un contrato mercantil, en un contrato de arrendamiento de servicios o equivalente. La Ley Orgánica exige un *contrato específico*. Esto no significa que deban firmarse dos contratos, nada impide que el contenido regulador que exige el artículo 12[12] LOPD, se incorpore como clausulado o anexo al contrato principal.

Cuando se *ceden* datos, o se *encomiendan servicios*, que suponen acceso a datos a entidades que los tratan en países distintos de los del Espacio Económico Europeo, se está realizando una *transferencia internacional* de datos personales, en este entorno, se considera que prestan un *nivel de protección adecuado* los Estados Miembros de la Unión Europea, los del Espacio Económico Europeo y los Estados respecto de los cuales la Comisión Europea haya declarado la existencia de un nivel adecuado de protección. Estos

---

[11] Artículo 11.2 de la LOPD: El consentimiento exigido no será preciso: a) Cuando la cesión está autorizada en una Ley; b) Cuando se trate de datos recogidos de fuentes accesibles al público; c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique; d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas; e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

[12] Artículo 12 de la LOPD: Acceso a los datos por cuenta de terceros: No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

últimos son Argentina, Canadá, Suiza, Gernesey, Isla de Man y Jersey. Estados Unidos se considera país seguro en supuestos específicos.

Por último, el Test de cumplimiento de LOPD pregunta por el nivel de seguridad de los ficheros, ante este conviene recordar que el artículo 81 del RDLOPD establece los *niveles de seguridad* que se aplicarán a los ficheros en *función de la tipología de datos* que contengan. El precepto identifica tres niveles[13], -básico, medio y alto-, para cada uno de los cuales fija las medidas a adoptar.

De igual forma el Test pregunta por la existencia de *Documento de Seguridad*[14] en la organización y los componentes de este: las *funciones y obligaciones del personal*, la adaptación de las medidas de seguridad de los productos software adquiridos o sobre el uso de soportes no informatizados para el tratamiento de datos de carácter personal.

En lo que respecta a la segunda parte de la herramienta EVALUA, la que corresponde al TEST de cumplimiento de medidas de seguridad este repasa las medidas adoptadas de acuerdo al nivel de protección que corresponda al fichero según el tipo de datos de carácter personal que trate.

Con carácter general, la *seguridad de la información* puede ser definida como la preservación de la confidencialidad, integridad y disponibilidad de la información y se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software.

---

[13] Niveles de seguridad: *1. Nivel Básico* (se aplica a todos los ficheros y tratamientos); *2. Nivel medio* (los relativos a la comisión de infracciones administrativas o penales; solvencia patrimonial y crédito; ficheros de Administraciones Tributarias que se relacionen con el ejercicio de sus potestades tributarias; ficheros de entidades financieras para finalidades relacionadas con la prestación de servicios financieros; ficheros de las Entidades Gestoras y Servicios Comunes de la Seguridad Social en relación con el ejercicio de sus competencias; ficheros de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social; aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos; también lo aplican, aunque deben incluir una medida de nivel alto, los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización. En ellos se aplicará, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto correspondiente al establecimiento de un registro de accesos); *3. Nivel alto* (ficheros con datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; ficheros que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas; aquéllos que contengan datos derivados de actos de violencia de género); *4. Excepciones* (los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos; los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando: los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros o bien se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad).

[14] Documento de seguridad, descrito en el Artículo 88 del RLOPD: recogerá las medidas de índole organizativa y técnica acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

La implantación de las medidas de seguridad es no solo algo recomendable para la generación de confianza, la protección del negocio y para la implantación de buenas prácticas de gestión, sino que, en el caso de España, tiene un carácter *obligatorio* en el marco de la protección de datos. En este sentido representa una obligación que la Directiva de protección de datos y, en el caso de España, la LOPD impone a los responsables de ficheros y a los encargados de tratamiento.

En este sentido, el artículo 9 de la LOPD, establece en su punto 1 que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las *medidas* de índole *técnica* y *organizativas* necesarias *que garanticen la seguridad de los datos de carácter personal* y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El RLOPD desarrolla las *medidas de seguridad*[15] en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias *para garantizar la seguridad* que deben reunir los ficheros, ya sean automatizados o manuales, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

A través de EVALUA se trataba de poner a disposición de los responsables de ficheros una herramienta que permitiese tanto *evaluar el cumplimiento* como, *facilitar el conocimiento de las medidas de seguridad*, tanto técnicas como organizativas, que es necesario implantar cuando se tratan datos de carácter personal.

Los objetivos que se han considerado al diseñar el cuestionario sobre medidas de seguridad disponible en la herramienta han sido facilitar la información más relevante sobre las medidas de seguridad obligatorias al tiempo que ofrecer una herramienta de autoevaluación; para ello, se ha tomado como base fundamental los contenidos incluidos en la *Guía de Seguridad,* en la que se recopila un cuadro resumen de las medidas de seguridad recogidas en el citado Título VIII del RLOPD, un modelo de *"Documento de Seguridad"*, que sirve de guía y facilita el desarrollo y cumplimiento de la normativa sobre protección de datos; en concreto se ha incluido en EVALUA, la lista de comprobaciones para realización de la auditoría de seguridad que se incluía en dicha Guía.

Además, la herramienta permite obtener, de modo análogo al descrito para el Test de cumplimiento de la LOPD, un informe con las deficiencias detectadas para, en su caso, adoptar las medidas correctoras correspondientes.

[15] Medidas de Seguridad: desarrolladas en el Título VIII del RLOPD (Artículos del 79 al 114).

En lo que respecta al inventario de ficheros y/o tratamientos de datos de carácter personal, y con el fin de poder evaluar el cumplimiento de las medidas de seguridad, sería necesario clasificar cada uno de los ficheros o tratamientos en el *nivel de medidas de seguridad* correspondiente, dependiendo del tipo de datos, colectivos y finalidad del tratamiento, de acuerdo a la clasificación descrita al hablar de niveles de seguridad en el Test de cumplimiento de LOPD.

Así mismo, será necesario determinar el *sistema de tratamiento* que se está realizando, es decir, el *modo en que se organiza la información*. Atendiendo al *sistema de tratamiento*, los sistemas podrán ser *automatizados*, *no automatizados* o *parcialmente automatizados*.

Las cuestiones planteadas en el Test, siguen el esquema de preguntas en torno al Documento de seguridad, su actualización y contenido, según proceda con respecto al nivel de seguridad que se esté analizando; así, de forma genérica, una vez chequeado el documento de seguridad se revisarán la existencia, puesta al día y adecuación de: las funciones y obligaciones del personal con respecto a los datos que está manejando, el registro de incidencias, el control de acceso a los sistemas, incluyendo la puesta al día de las listas de usuarios, la gestión de soportes y documentos, los procesos de identificación ante el sistema y de autenticación, procesos de copias de respaldo y recuperación de datos informatizados, el registro de accesos al sistema (únicamente adecuado para ficheros de nivel alto), la delegación de autorizaciones, repaso del régimen de trabajo fuera de los locales de la ubicación del fichero, encargado del tratamiento, si lo hubiera, prestación de servicios sin acceso a datos personales, ficheros temporales o copias de trabajo, acceso a datos a través de redes de comunicaciones, auditoría, criterios de archivo, almacenamiento de la información, custodia de soportes; esto es, todos aquellos aspecto que el ya descrito Titulo VIII del RLOPD tiene en cuenta al hablar de *medidas de seguridad*.

FORMA DE TRABAJO

EVALUA se estructura en base a todos los conceptos indicados en el apartado anterior (tanto de LOPD como de Medidas de seguridad), a través de un conjunto de Test que permiten, además de hacer reflexionar al ejecutante sobre el estado de estas cuestiones sobre el sistema a analizar, almacenar la información necesaria para la posterior recepción del producto *informe/s final/es*.

Así, y en lo que respecta al TEST cumplimiento de LOPD el usuario comienza con cuestiones del tipo: con la información de la que dispone actualmente ¿cree que Vd. o su empresa realizan tratamientos de datos de carácter personal?, si Vd. trata datos personales ¿los incluye en ficheros? ¿Se han notificado los ficheros a la AEPD para su inscripción en el Registro General de Protección de Datos? Cuestiones que pretenden llevarle a la reflexión sobre si está tratando o no datos de carácter personal, en base a

que y porqué, y en que forma se recogen, almacenan, tratan, se cumple con las obligaciones sobre el sujeto objeto y si se cumplen los principios que la Ley indica.

Las preguntas propuestas pretenden, de un modo práctico, verificar el cumplimiento de los principios a atender y obligaciones a cumplir en una organización.

En lo que respecta a la segunda parte de la herramienta EVALUA, la que corresponde al TEST cumplimiento medidas de seguridad la herramienta estructura sobre la pregunta básica del nivel de medidas de seguridad a evaluar (básico, medio o alto) y en base a él establece el esquema de cuestiones a plantear que dependiendo del nivel a evaluar genera un ciclo de diferentes pasos.

En función de las respuestas proporcionadas, la herramienta le presentará las preguntas relacionadas con el nivel de medidas de seguridad y el sistema de tratamiento. Atendiendo al sistema de tratamiento, vemos que hay un grupo de apartados que son comunes a los tres sistemas de tratamiento. Algunos de estos apartados incluyen medidas de seguridad de nivel básico, y algunos de estos apartados incluyen también medidas específicas para los ficheros clasificados de nivel medio. Este es el caso de las medidas y controles relativos al Documento de seguridad, el Registro de incidencias, la gestión de soportes y documentos que incluyen medidas tanto para el nivel básico como del nivel medio.

Por lo que respecta a los ficheros automatizados, además de los apartados comunes, el Reglamento de desarrollo de la LOPD establece medidas específicas tanto para los ficheros clasificados como de nivel básico o alto. Lo mismo ocurre con los ficheros no automatizados o manuales ya que igualmente cuentan con medidas específicas tanto para los ficheros de nivel básico como de nivel alto.

Obviamente la herramienta de autoevaluación de medidas de seguridad debía permitir evaluar todas estas especifidades. Una vez que se contestan las preguntas iniciales la herramienta presentará las preguntas, agrupadas en los apartados correspondientes al nivel de medidas de seguridad y al sistema de tratamiento.

En ambos casos debe entenderse que la utilización de esta herramienta como guía de ayuda para evaluar el cumplimiento de la LOPD y de las medidas de seguridad que deben implantarse en los ficheros y tratamientos con datos de carácter personal, debe, en todo caso, tener en cuenta los aspectos y circunstancias aplicables en cada caso concreto, sin prejuzgar el criterio de la Agencia Española de Protección de Datos en el ejercicio de sus funciones. Y, como se señalaba antes, el responsable podrá optar por realizar una encuesta para un fichero específico, o por realizar un test más amplio que englobe a la totalidad de los ficheros.

PRODUCTOS A OBTENER

Cada uno de los TEST disponibles (cumplimiento de la LOPD o cumplimiento medidas de seguridad) proporciona un informe final basado en las respuestas facilitadas.

Este informe, en formato PDF, que no vincula a la Agencia Española de Protección de Datos y que puede recuperarse de igual forma que se realizaba la continuación del test, formula recomendaciones de actuación en su ámbito.

En cada uno de los informes resultado que la herramienta EVALUA presenta como resultado del Test correspondiente se incluyen, a modo de Anexos , los recursos que la Agencia pone a disposición así como el conjunto de definiciones que correspondan al ámbito (cumplimiento LOPD o seguridad LOPD).

El *informe* de autoevaluación del *cumplimiento de la LOPD* se estructura en distintos apartados que abarcan los distintos capítulos de la Ley: identificación de ficheros y tratamientos, información y consentimiento, principios que rigen el tratamiento de los datos personales, derechos de acceso, rectificación, cancelación y oposición, relaciones con terceros, transferencia internacional de datos, encargado de tratamiento y seguridad;

Por cada apartado el informe de autoevaluación mostrara la descripción de lo estipulado por la LOPD para su cumplimiento y los resultados de la autoevaluación con indicación de las deficiencias detectadas

Por su parte, el *informe* correspondiente a evaluación de *cumplimiento de medidas de seguridad* contiene: una introducción con Información de carácter general, el objeto y el alcance del informe, información sobre los tipos de medidas de seguridad a implantar dependiendo de la clasificación por niveles establecida en el Reglamento de desarrollo de la LOPD.

De forma análoga a lo descrito para el Test de cumplimiento de la LOPD, por cada apartado el informe de autoevaluación mostrara la descripción de las medidas de seguridad que han de implantarse en cada apartado y los resultados de la autoevaluación con indicación de las deficiencias detectadas