economistas
Consejo General

ReDigital economía y transformación digital

REA auditores

FICHA 03 22

grupo de trabajo de auditoría

OCTUBRE 2022

La transformación digital llevada a cabo por las entidades auditadas exige una evolución en el mismo sentido de los auditores de cuentas con objeto de incrementar la calidad de los trabajos, evaluar mejor los riesgos cada vez más amplios de las entidades auditadas, mejorar la eficiencia del trabajo al reducir tareas de poco valor y desplegar acciones que permitan captar y retener el talento.

Respecto al cumplimiento normativo, se han introducido importantes requerimientos en el Reglamento de la Ley de Auditoría que afectan a la forma de trabajar de los auditores a partir del 1 de julio de 2022. Citamos algunos de ellos: la obligación de que todos los papeles de trabajo sean en formato electrónico, con las debidas medidas de seguridad que garanticen su autenticidad; la digitalización de toda la documentación existente en formato papel; procedimientos que aseguren la custodia, integridad y recuperación de la información; garantizar la accesibilidad y autorización restringida para su acceso; y realizar de forma rutinaria copias de seguridad en formato digital en diferentes momentos y, al menos, una vez al año. Todos ellos son retos a los que se enfrenta la actividad profesional.

Se observa, por lo tanto, una exigencia de modernización tecnológica de los despachos de auditoría que es prioritaria y estratégica, teniendo en cuenta la función de interés público de la actividad profesional de la auditoría de cuentas.

Desde el grupo de trabajo de auditoría de ReDigital publicaremos periódicamente estas fichas para ayudar a los auditores de cuentas a cumplir con la normativa y, a su vez, mejorar la eficiencia y eficacia en su trabajo diario.

# Medidas informáticas y de otro tipo en relación con el tratamiento de datos personales

Como continuación de las fichas 1 y 2 anteriores, el tratamiento de datos personales supone el último apartado de los procedimientos administrativos relativos a la identificación, valoración y respuesta a los riesgos que puedan afectar a la actividad de auditoría de cuentas.

El artículo 74 del **Real Decreto 2/2021,** de 12 de enero, por el que se aprueba el Reglamento de desarrollo de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, desglosa las obligaciones de los auditores de cuentas en relación a la protección de datos de carácter personal, que se extienden a los terceros afectados, en el caso de que los auditores de cuentas externalicen las actividades de auditoría.

El tratamiento de datos de carácter personal llevado a cabo por los auditores de cuentas como consecuencia del ejercicio de su actividad, incluido el de los datos contenidos en los documentos o papeles de trabajo utilizados para tal fin, se encuentra sometido a lo dispuesto 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 la **Ley Orgánica 3/2018**, de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales y sus disposiciones de desarrollo

Teniendo en cuenta lo anterior, **están obligados a cumplir la normativa de protección de datos de carácter personal todas las personas, empresas y entidades públicas y privadas que utilicen cualquier dato personal en el desarrollo de sus actividades.**

## ALGUNAS DEFINICIONES

- **Dato de Carácter Personal:** Toda información sobre una persona física identificada o identificable (artículo 4.1 RGPD).
- **Persona física:** Toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (artículo 4.1 RGPD).

- **Tratamiento de datos:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción (artículo 4.2 RGPD).
- **Afectado o Interesado:** Persona física titular de los datos que sean objeto de tratamiento.
- **El Responsable del tratamiento** es el sujeto obligado a cumplir todas las disposiciones del RGPD con el deber de tratar los datos personales de manera lícita y aplicar las medidas adecuadas para protegerlos en cualquier fase del tratamiento.
- **El Encargado del tratamiento** o encargado es la persona física o jurídica, autoridad, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

## MANUAL DE ORGANIZACIÓN INTERNA (MOI) REA AUDITORES

El procedimiento que recoge el MOI relativo al riesgo sobre el tratamiento de datos personales establece la necesidad de disponer de un Manual RGPD que identifique y detalle las medidas de salvaguarda y los procedimientos que tiene implantados la Firma para mitigar los riesgos sobre el tratamiento de datos personales. A modo de guía se deberá tener en cuenta lo siguiente:

- **El auditor de cuentas es responsable del tratamiento de datos de carácter personal que le pueden ser proporcionados por la entidad auditada**. Se debe comprometer a tratar los datos exclusivamente para llevar a cabo la prestación del servicio de auditoría, así como para dar cumplimiento a cualesquiera obligaciones legales derivadas de su condición de auditor.
- **Los datos de carácter personal tendrán carácter confidencial** sobre la base de la obligación de secreto profesional regulada, entre otras, en la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, sin perjuicio de eventuales requerimientos que emanen de nuestro ordenamiento jurídico, por acatamiento de cualquier disposición o resolución de cualquier autoridad administrativa o reguladora y en todo caso por requerimiento de tribunales o la autoridad de control.
- **El auditor de cuentas debe dar cumplimiento a las obligaciones que le son impuestas por la normativa de protección de datos vigente,** y adoptará las medidas de seguridad oportunas habida cuenta del estado de la tecnología, los costes de aplicación, la naturaleza, alcance, contexto y los fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas, garantizando el cumplimiento de las obligaciones establecidas en los artículos 32 a 34 del RGPD en relación con los datos tratados.
- **El auditor de cuentas debe implementar las medidas oportunas para atender, en tiempo y forma, las posibles peticiones de ejercicio de derechos que formulen los interesados.** Adicionalmente, si recibiera de un interesado una solicitud para el ejercicio de un derecho de rectificación, supresión o limitación del tratamiento, pondrá tal circunstancia en conocimiento de la otra parte contratante de manera inmediata.
- **El auditor de cuentas conservará aquellos datos que sean estrictamente necesarios** de conformidad con lo establecido en la Ley de Auditoría de Cuentas 22/2015, de 20 de julio, **para poder justificar la prestación de sus servicios profesionales,** para el caso de que la misma fuera cuestionada y el tiempo de prescripción legalmente establecido.
- **Los riesgos de tratamiento de datos personales pueden ser incorporados a la matriz global de riesgos del auditor, o bien pueden constituir una matriz específica y concreta** sobre este tipo de riesgos para facilitar su seguimiento. A modo de ejemplo, se enumeran en el Registro 103, disponible como Anexo de esta Ficha, los primeros riesgos que se obtienen de la lectura detallada de la normativa.
- Los riesgos del Registro 103 son los propios que corresponden a un gestor de datos personales (los del propio personal de la firma auditora), aunque, tal como se ha mencionado, también conviene identificar los riesgos atribuibles al auditor como responsable de los datos de sus clientes.
- En el Registro de actividades de tratamiento (RAT) de la firma de auditoría debe figurar la respuesta de la Firma a los riesgos.

## CONSECUENCIAS DEL INCUMPLIMIENTO DE LA NORMATIVA

**El incumplimiento de la normativa sobre protección de datos puede acarrear cuantiosas multas, incluso responsabilidad penal.**

Así el afectado o interesado que haya sufrido un perjuicio, material o inmaterial, como consecuencia de una operación de tratamiento de datos que no se atenga a la normativa de protección de datos, tiene la potestad de presentar una reclamación ante la AEPD, sin perjuicio del derecho de indemnización que el Interesado pudiera reclamar judicialmente.

Dependiendo del artículo del Reglamento General de Protección de Datos que haya sido vulnerado las sanciones impuestas pueden ascender de los 10 millones de euros o el 2% como máximo del volumen de negocio total anual global hasta los 20 millones de euros o el 4% como máximo del volumen de negocio total anual global (artículo 83 RGPD).

Desde la perspectiva de la normativa reguladora de la actividad de auditoría de cuentas se impone a los auditores de cuentas la obligación de aplicar lo establecido en la normativa de protección de datos personales cuando, en el desarrollo de un trabajo de auditoría de cuentas, se traten datos personales, sin que, por otra parte, dicha normativa de protección de datos personales pueda impedir la aplicación de lo exigido por la normativa de auditoría de cuentas., conforme a la Consulta de auditoría nº 2 del BOICAC 120, de diciembre de 2019, publicada en la página web del ICAC el 20 de diciembre de 2019.

En este sentido, la Agencia Española de Protección de Datos (autoridad supervisora de esta materia en España) confirma que los auditores de cuentas, como cualquier otra persona física o jurídica, están sometidos a la normativa reguladora de protección de datos cuando, en la realización de sus trabajos de auditoría de cuentas, traten datos de carácter de personal, de conformidad con las definiciones de "datos personales" y "tratamiento" establecidas en el artículo 4, apartados 1 y 2, del RGPD, respectivamente. Y en estos casos, la sujeción de los auditores de cuentas a la normativa reguladora de protección de datos lo será en calidad de **"responsables de tratamiento"**.

A los efectos del art. 74 del RLAC, los auditores de cuentas deberán adoptar las medidas de organización interna necesarias para dar cumplimiento a las obligaciones derivadas de la aplicación de la normativa sobre protección de datos en el desarrollo de sus trabajos de auditoría de cuentas para proteger los intereses y derechos de los interesados, y sin que lo dispuesto en la normativa de protección de datos, o en la de confidencialidad y secreto profesional, pueda aducirse como impedimento a la aplicación de lo exigido por la normativa reguladora de la actividad de auditoría de cuentas. A estos efectos, el tratamiento de los datos debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos para lo cual deben establecerse medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

## PRINCIPALES ASPECTOS A CONSIDERAR EN LA APLICACIÓN DEL RGPD Y LA LOPDGDD

El siguiente gráfico resume los principales ámbitos relacionados con RGPD y LOPDGDD


La **Agencia Española de Protección de Datos** dispone en su página web numerosas guías, que indican los criterios a seguir en los distintos aspectos de la aplicación de la normativa de protección de datos

para su adecuado cumplimiento entre las que se encuentra la *Guía del RGPD para responsables del tratamiento* que puede facilitar al auditor de cuentas el cumplimento de la normativa en su calidad de responsable y en concreto una hoja de ruta a seguir para la adaptación al RGPD.

### GUÍAS DE REFERENCIA DE LA AEPD[1]:

- Guía del Reglamento General de Protección de Datos para Responsable de Tratamiento.
- Gestión del riesgo y evaluación de impacto en tratamientos de datos personales.
- Guía para la notificación de brechas de datos personales.
- Guía de Privacidad desde el Diseño.
- Guía de Protección de Datos por Defecto.
- Protección de Datos por Defecto: Listado de medidas.
- Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo.

### GUÍAS DE REFERENCIA DE REA AUDITORES-CGE:

- MOI REA Auditores

1. https://www.aepd.es/es/guias-y-herramientas/guias

## ANEXO. - REGISTRO 103 TRATAMIENTO DE DATOS PERSONALES

| RIESGOS IDENTIFICADOS RGDP |
|---|
| Denominación del riesgo |
| Tratar datos personales cuando no es necesario para la finalidad perseguida. |
| Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales. |
| Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales. |
| Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión. |
| Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas. |
| Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento. |
| Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros. |
| Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias. |
| Utilizar cookies de seguimiento u otros mecanismos de rastreo sin obtener un consentimiento válido tras una información adecuada. |
| Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia. |
| Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados. |
| No obtención de las autorizaciones legales necesarias. |
| Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe notificarse la creación, modificación o cancelación de un tratamiento de datos personales a la AEPD o a la autoridad de protección de datos competente. |
| Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (cookies, ubicación geográfica, comportamiento, hábitos de navegación, etc.) |
| En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas). |
| Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales. |
| Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad. |
| No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos ARCOPL realizados ante los encargados de tratamiento. |
| Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato. |
| Dificultar o imposibilitar el ejercicio de los derechos ARCOPL. |
| Carencia de procedimientos y herramientas para la gestión de los derechos ARCOPL. |
| Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales. |
| Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización. |
| ... |