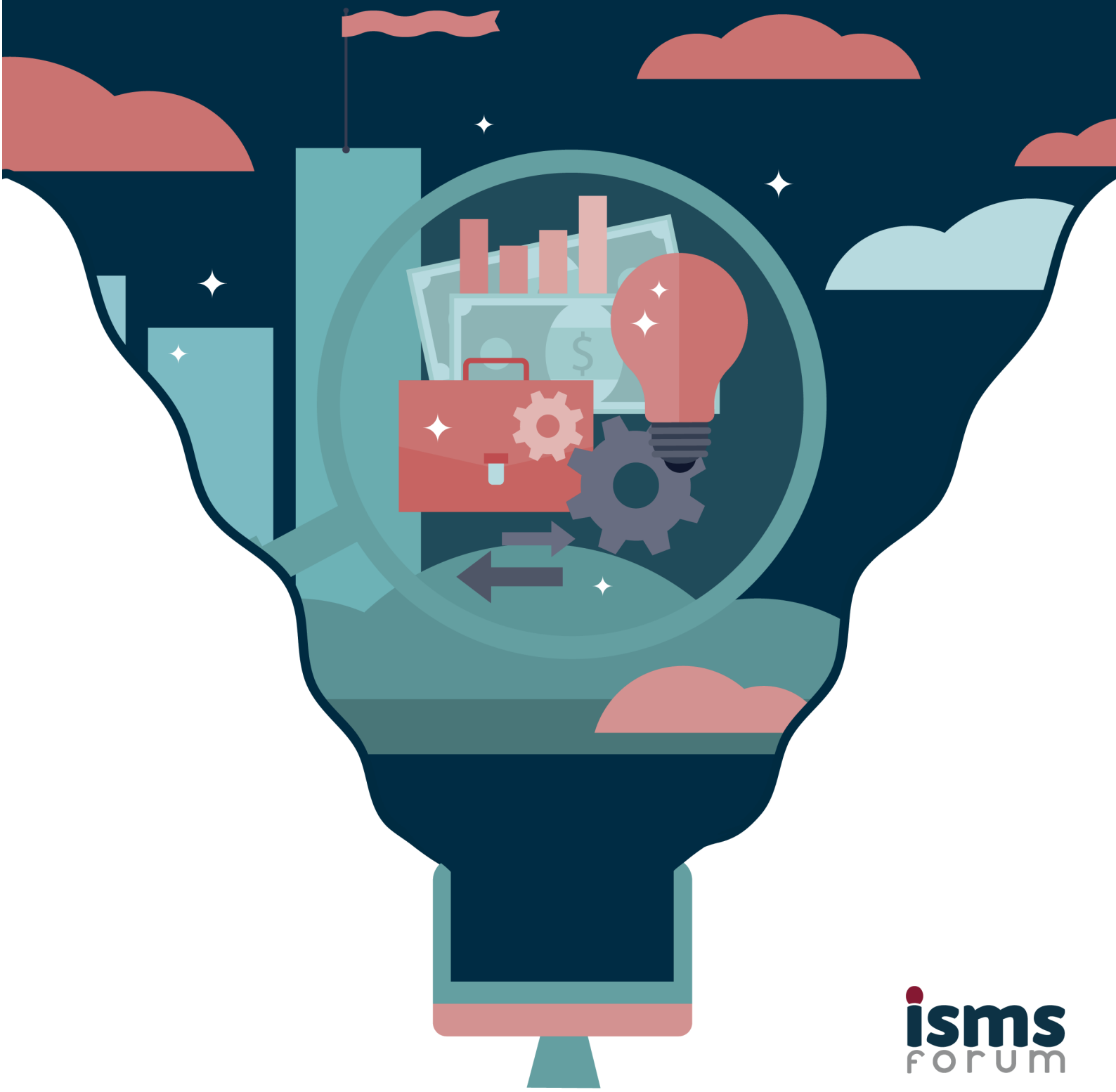
GUÍA DE BUENAS PRÁCTICAS EN AUDITORÍAS RGPD



isms forum

GUÍA DE BUENAS PRÁCTICAS EN AUDITORÍAS RGPD

Con la participación de los siguientes profesionales y organizaciones:

Coordinación:

Esmeralda Saracíbar
Esther García
Gemma Déler
Henry Velásquez
Josep Bardallo
María Jesús Morena
Patricia Muleiro
Ramón Miralles

Colaboradores:

Carlos Díaz
Cecilio Criado
Francisco Rodríguez
Javier Lomas
Javier Rubio
Juan Prieto
Laura del Carre
Maica Aguilar
Manel Leal
María de la Torre
Óscar López
Pablo Martínez
Paula Armentia
Xavier Vila

Editor:

Daniel García Sánchez, Director General de ISMS Forum

Diseño y maquetación:

Raquel García Robles, Asistente de comunicación de ISMS Forum

isms forum

Índice

isms forum

ÍNDICE

ÍNDICE

01

Introducción

La entrada en vigor del 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, también denominado Reglamento General de Protección de Datos o RGPD) ha supuesto un cambio radical en la forma en la que las organizaciones deben cumplir con sus obligaciones en materia de protección de datos personales. En este entorno, las empresas y administraciones públicas se han encontrado con un claro cambio de paradigma respecto a la normativa anterior de protección de datos, siendo ahora las propias organizaciones las que deben diseñar y evaluar las medidas necesarias para garantizar el cumplimiento con la normativa en cuestión.

Como en cualquier otro marco de gestión del cumplimiento, las auditorías son una parte esencial de los procesos de revisión y mejora continua. En lo que respecta a las auditorías de protección de datos, en el marco normativo vigente, las organizaciones están viviendo procesos de auditoría dispares en cuanto a varios elementos esenciales de cualquier proyecto de auditoría como es el alcance, la periodicidad o el enfoque del mismo.

En este entorno, surge la iniciativa de la DPD Community de ISMS Forum (International Information Security Community) de elaborar y publicar una Guía de Buenas Prácticas en Auditorías RGPD que arroje unas pautas orientativas ante este tipo de iniciativas.

Ahora bien, como ya se ha indicado, a diferencia de la normativa anterior de protección de datos, el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, también LOPDGDD) no establecen una obligación explícita para los responsables del tratamiento de realizar auditorías de cumplimiento de la normativa de protección de datos.

No obstante, el RGPD introduce como uno de sus principios rectores (artículo 5.2.) el principio de responsabilidad proactiva ("accountability"), indicando que el responsable del tratamiento será no solo responsable de cumplir con los principios del RGPD, sino que también deberá ser capaz de demostrarlo. En este sentido, resulta necesario disponer de evidencias de cumplimiento, que generalmente requerirán documentar de forma adecuada todas las medidas implementadas con la finalidad de dar cumplimiento a las obligaciones establecidas en la normativa de protección de datos.

Sin perjuicio del principio de responsabilidad proactiva, el RGPD dispone en su artículo 24.1

que el responsable del tratamiento revisará las medidas técnicas y organizativas que haya adoptado con el fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, a lo que se une lo que establece el artículo 32.1.d sobre la necesidad de establecer un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas implementadas por el responsable o el encargado a fin de garantizar la seguridad del tratamiento, viéndose reforzado este concepto en las disposiciones relativas a Encargados del Tratamiento (artículo 28), Normas corporativas vinculantes (artículo 47.j) y Códigos de conducta (artículo 40). De acuerdo con las citadas disposiciones, se desprende la intención del legislador no solo de transmitir la necesidad de realizar auditorías sino también de establecer un marco de revisión continua de cumplimiento normativo en materia de protección de datos, siendo la auditoría uno de los mecanismos de verificación más adecuados para implementar dicho proceso.

En línea con la orientación a riesgos que viene a introducir el RGPD, las organizaciones han de tener presente el nivel del riesgo correspondiente a cada actividad de tratamiento a la hora de realizar auditorías de protección de datos. No obstante, dicho planteamiento deja al criterio de cada responsable del tratamiento algunos de los aspectos clave relativos a la realización de auditorías. En este sentido, los responsables del tratamiento se encuentran ante supuestos que en la anterior normativa de protección de datos venían expresamente regulados.

En primer lugar, se plantea la problemática del alcance de la auditoría. Mientras que la normativa anterior establecía la obligación de auditar el cumplimiento de determinadas disposiciones relativas exclusivamente a las medidas de seguridad del tratamiento, en el marco de una auditoría de cumplimiento de RGPD, ha de evaluarse tanto el cumplimiento de la organización con las disposiciones que establecen obligaciones relativas a medidas de seguridad adecuadas al riesgo que el tratamiento implica para los derechos y libertades de los interesados, como el cumplimiento con las obligaciones restantes que requieren la implementación de medidas de carácter jurídico y organizativo. En este sentido, los responsables del tratamiento se encuentran ante la necesidad de elaborar nuevos controles de auditoría y los correspondientes indicadores de cumplimiento a fin de poder evaluar el grado de cumplimiento de las organizaciones en lo que respecta a las obligaciones de carácter jurídico – organizativas.

Del mismo modo, la normativa anterior establecía una periodicidad de dos años para auditar los sistemas de información e instalaciones de tratamiento y almacenamiento de datos para aquellos tratamientos que, en al anterior modelo de seguridad de los datos, requerían de la implantación de medidas de seguridad de los denominados niveles medio y alto. Como se ha indicado anteriormente, el RGPD no viene a establecer la periodicidad de auditorías de protección de datos, sino que traslada la obligación a cada responsable del tratamiento de evaluar el riesgo inherente a las actividades del tratamiento que realiza, para que, conforme a dicho nivel de riesgo, implemente las medidas de control más adecuadas, entre ellas la auditoría, con la periodicidad que considere más adecuada al riesgo.

02

Objetivos

En este contexto de falta de directrices y orientaciones específicas, el principal objetivo de esta Guía es establecer una serie de pautas generales para los responsables del tratamiento en relación con la realización de auditorías de cumplimiento con la normativa vigente de protección de datos; unas pautas que, en su caso, también pueden ser aplicadas por encargados del tratamiento.

En primer lugar, se pretende dar respuesta a las dudas más frecuentes de los responsables del tratamiento, en particular, relativas a la necesidad de realización de auditorías, las obligaciones que forman parte del alcance de la auditoría y la periodicidad de realización de las auditorías. En esta línea, se analizarán las diferencias y la correlación entre auditorías RGPD y los controles periódicos de cumplimiento que realizan las organizaciones, de igual forma que se darán pautas generales en relación con la figura del auditor realizándose una comparativa entre las características de auditoría interna y auditoría externa en el marco de un proyecto de auditoría RGPD.

La Guía se estructura conforme a las fases que se han considerado necesarias en un proyecto de auditoría RGPD. Como en cualquier proyecto de auditoría, la primera fase consistirá en la determinación del alcance y planificación, seguida por la obtención de evidencias. Se analizarán las características necesarias para que una evidencia pueda considerarse adecuada para acreditar el cumplimiento con una determinada obligación. Del mismo modo, se introducirán los métodos recomendados para la adecuada e imparcial obtención de las evidencias.

En lo relativo a la segunda fase de la auditoría RGPD, se expondrán los criterios que se consideran relevantes a la hora de valorar las evidencias obtenidas y, por otro lado, se especificarán recomendaciones sobre métodos de cálculo del grado de cumplimiento con las obligaciones del RGPD.

Finalmente, se analizarán los requisitos necesarios para la tercera fase de la auditoría RGPD, consistente en la elaboración del Informe de Auditoría y del correspondiente Plan de Acción. Se detallarán los elementos necesarios para la elaboración de cada uno de estos documentos, así como las recomendaciones relativas a la comunicación de los resultados de la auditoría a las partes relevantes dentro de la organización.

Como en cualquier proyecto relacionado con el tratamiento de datos en las organizaciones, será imprescindible el liderazgo y colaboración de los Delegados de Protección de Datos en la realización de auditorías RGPD. En este sentido, la presente Guía ha de servir tanto a los Delegados de Protección de Datos como al resto de los profesionales del sector de protección de datos y responsables de cumplimiento normativo, para que pueden lograr un mayor grado de cumplimiento de sus organizaciones en materia de protección de datos a través de una adecuada realización de auditorías RGPD.

03

Aspectos esenciales de la Auditoría RGPD

isms forum

El pasado 25 de mayo de 2018 resultaba de aplicación el RGPD que venía a derogar la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. La entrada en vigor del RGPD producía un cambio fundamental, a nivel europeo, en la forma que las organizaciones tenían de gestionar el cumplimiento normativo en materia de protección de datos personales.

En España, dicho impacto se trasladaba a la legislación interna con la promulgación de nueva LOPDGDD que derogaba el régimen anterior compuesto, principalmente por la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante, LOPD) y el Reglamento de desarrollo de la mencionada Ley Orgánica, el Real Decreto 1720/2007, por el que se aprueba el Reglamento de Desarrollo de la LOPD (en adelante, el RLOPD).

Dicho régimen había proporcionado una guía certera para responsables y encargados del tratamiento al recoger una definición clara de las medidas que las organizaciones debían adoptar e implementar para cumplir con los principios reguladores de la protección de datos personales.

En relación con la realización de auditorías, el RLOPD concretaba su obligatoriedad en el artículo 96 cuando contemplaba que:

> *A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.*

Se constituían así las auditorías bienales en una herramienta fundamental para determinar el grado de cumplimiento de las organizaciones en esta materia, si bien centrando la verificación del cumplimiento exclusivamente en las medidas de seguridad.

En el nuevo contexto normativo, responsables y encargados del tratamiento, así como profesionales del sector se vienen preguntando -entre otras cuestiones- si la realización de auditorías en protección de datos sigue siendo una obligación o no y, para el caso de que lo fuera o de que fuese recomendable, cuál debería ser su alcance, enfoque o periodicidad.

Como veremos en los siguientes apartados, si bien no existe un artículo concreto que establezca dicha obligación ni en el RGPD ni en la LOPDGDD, la realización de auditorías en materia de protección de datos resulta, en el marco de los principios de responsabilidad proactiva y enfoque a riesgos, necesaria y muy recomendable.

3.1. Necesidad y nuevo paradigma

¿Exige el nuevo contexto normativo la obligación de realizar de auditorías de protección de datos?

Pues bien, si nos atenemos al tenor literal del RGPD, encontramos menciones a la realización de auditorías en el ámbito de:

- Los encargados del tratamiento: cuando en el artículo 28.3.h se establece la obligación de los mismos de poner a disposición de los responsables la información necesaria para demostrar el cumplimiento de sus obligaciones y, en consecuencia, les obliga a: *contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable*.

- El DPD y sus funciones: cuando, en el artículo 39, al detallar la función de supervisión del cumplimiento de la normativa de protección de datos por el DPD establece que ello incluirá: *la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes*.

- Las Normas corporativas vinculantes: cuando al establecer el contenido de las mismas se refiere a que incluirán los mecanismos que permitan garantizar la verificación de su cumplimiento y especifica que: *dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado*. Añade este apartado del RGPD que: *los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite*.

- En cuanto a la LOPDGDD la única referencia que se incluye a la auditoría se circunscribe a los poderes de investigación de las autoridades de protección de datos y se concreta en los planes de auditoría preventiva que puede llevar a cabo la Agencia Española de Protección de Datos (AEPD) a los efectos de analizar el cumplimiento de la normativa de protección de datos por parte de un sector o de un responsable (artículo 54).

De esta primera lectura literal y formalista del RGPD y de la LOPDGDD podemos concluir que no existe una obligación explicita a la realización de auditorías si bien las mismas se

presentan como una de las herramientas para verificar y, en su caso, poder demostrar el cumplimiento de la normativa de protección de datos por parte de los encargados hacia los responsables, de los propios responsables (cuando se dotan de DPD o de normas corporativas vinculantes) o de las propias autoridades de protección de datos.

Cabe en todo caso mencionar que, en los primeros borradores del RGPD, se disponía que el responsable del tratamiento debía implementar mecanismos para verificar la eficacia de las medidas adoptadas, y que siempre que no fuera desproporcionado, tales verificaciones serían "llevadas a cabo por auditores independientes internos o externos", por tanto, haciéndose una referencia directa a actividades de auditoría como técnica de verificación del cumplimiento.

Sin perjuicio de lo dicho hasta el momento, resulta relevante -antes de concluir sobre la obligatoriedad o no de realizar esas auditorías- analizar en profundidad las previsiones de los artículos 24 y 32 del RGPD, ya que, aunque los mismos no incluyen menciones a la realización de auditorías, dichos artículos contienen los principios (responsabilidad proactiva y enfoque a riesgos) que han reconfigurado la normativa de protección de datos en la Unión Europea.

3.2. Responsabilidad proactiva y enfoque a riesgos

Como se ha indicado anteriormente, el RGPD ha marcado un antes y un después en materia de protección de datos, regulando una nueva forma de gestionar el cumplimiento. Si bien, la nueva norma, regula diferentes tipos de medidas para conseguir su cumplimiento, es destacable que ahora el regulador hace descansar, en las propias organizaciones, el diseño e implementación de aquellas medidas que cada una de ellas, a la vista de su propia estructura, tipo de negocio o contexto, considere más convenientes para lograr el cumplimiento de la norma.

En este sentido se pronuncian el considerando 74 y los artículos 5.2 y 24.1 del RGPD y la LOPDGDD que incluye, en el Título V de su texto, un Capítulo I bajo el epígrafe Disposiciones generales, medidas de responsabilidad activa a través del cual se da entrada y se regula el alcance de la responsabilidad de las organizaciones en el cumplimiento de la norma.

Así, el considerando 74 del RGPD establece:

Debe quedar establecida la responsabilidad del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe ***estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas.*** *Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.*

Por su parte, los artículos 5.2. y 24.1 del mismo texto legal, se pronuncian en similares términos:

Artículo 5.2. RGPD:

El responsable del tratamiento será ***responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo*** *("responsabilidad proactiva").*

Artículo 24.1:

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

En la misma línea apuntada, el artículo 28 de la LOPDGDD en su apartado 1 establece la responsabilidad de la implantación de medidas técnicas y organizativas apropiadas para el cumplimiento de la norma y la acreditación de su cumplimiento tanto en el responsable como en el encargado del tratamiento, continuando en su apartado 2 y resto del Capítulo I -antes citado- con la enumeración de diferentes situaciones de riesgo que las organizaciones deberán tener en cuenta a la hora de diseñar y adoptar dichas medidas.

Por otro lado, el artículo 32. del RGPD establece la necesidad de "verificación y evaluación" de las medidas técnicas implementadas por el responsable:

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 riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

(...) d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Nos encontramos, por tanto, con un principio que establece para los responsables y encargados la **obligación "proactiva" del cumplimiento de la norma y ello a través de la implantación de medidas técnicas y organizativas que sean apropiadas. Dichas medidas además deben ser revisadas y actualizadas cuando se considere necesario**.

La nueva regulación, en definitiva, busca el cumplimiento de la norma con antelación (y desde la prevención) para evitar que se produzca cualquier infracción de los derechos o libertades del interesado.

Durante la Guía se ha confirmado que el principio de responsabilidad proactiva o principio de accountability hace recaer en el responsable o encargado la responsabilidad de (i) implantar aquellas medidas que sean las precisas para garantizar el cumplimiento de la norma; (ii) demostrar el cumplimiento y, por lo tanto, la eficacia de las medidas adoptadas y (iii) revisar y actualizar dichas medidas.

A la vista de lo anterior, quedaría ahora determinar cómo una organización puede llegar a determinar qué medidas son las apropiadas para el cumplimiento de la norma.

En este punto es importante volver a recordar el antes citado artículo 24 del RGPD el cual considera como base para la determinación de las medidas a implantar lo siguiente: *(...) dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como* ***el riesgo para los derechos y libertades de las personas físicas***. Nos encontramos, por tanto, con un cumplimiento enfocado a riesgos, el cual igualmente se repite en los considerandos 75 a 77.

Así, el considerando 75 del RGPD incluye una enumeración de aquellos tratamientos de datos que, con carácter general, pueden ser considerados de riesgo para los derechos y libertades de los interesados:

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a:

- *Problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.*

- *Casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos.*

- *Casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual o las condenas e infracciones penales o medidas de seguridad conexas.*

- *Casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales.*

- *Casos en los que se traten datos personales de personas vulnerables, en particular niños.*

- *Casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.*

Por su parte, el considerando 76 dice que:

La probabilidad y gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

En base a todo lo expuesto, podemos concluir que el cumplimiento de la normativa de protección de datos personales se basa en un enfoque de aproximación al riesgo, pero no a cualquier tipo riesgo, sino al derivado de la protección de los derechos y libertades de las personas físicas. Ello hace que las organizaciones deban realizar, con anterioridad al diseño e implementación de estas medidas, una valoración de dicho riesgo teniendo en cuenta diferentes factores, como por ejemplo la naturaleza, el ámbito, el

contexto y los fines del tratamiento.

Consecuentemente, nos vamos a encontrar con diferentes tipos de medidas para distintos modelos de organizaciones. En base al principio de accountability o responsabilidad proactiva, cada una de ellas, deberá implementar aquellas reglas o medidas que le permitan cumplir con la norma y, además, demostrar que son las más adecuadas para que sus procesos, políticas y procedimientos estén alineados con el cumplimiento de la norma.

Como obligación adicional, las organizaciones no deberán olvidar revisar dichas medidas siempre que las circunstancias y por ende, los tratamientos y sus finalidades pudieran verse modificados a fin de ajustar aquellas a la nueva valoración de riesgo que deberán llevar a cabo.

A mayor abundamiento, cabe indicar que la AEPD en su 10ª Sesión Anual Abierta[1] señaló que, bajo la nueva normativa, las auditorías no son preceptivas pero si necesarias. Por tanto, nos encontramos en un entorno normativo en el que la obligación proactiva de cumplimiento con la normativa implica la necesidad de realización de auditorías de cumplimiento.

En conclusión, en el cumplimiento de los principios de responsabilidad proactiva y enfoque a riesgos expuestos, las organizaciones deberán:

1. Haber implantado las medidas que consideren necesarias para garantizar que cumplen con la normativa de protección de datos.

2. Estar en disposición de acreditar que cumplen la norma (lo que incluye la eficacia de las medidas implantadas).

3. Realizar revisiones y actualizaciones de dichas medidas.

Llegados a este punto, no podemos sino concluir que, las auditorías se configuran como la herramienta en la que instrumentalizar esa revisión periódica y continua que permite a las organizaciones, en todo momento, asegurarse (por verificación) del cumplimiento de la norma y, llegado el momento, poder demostrarlo.

[1] https://www.aepd.es/sites/default/files/2019-12/9-preguntas.pdf

3.3. Beneficios de la realización de Auditorías

Concluida la necesidad de llevar a cabo auditorías o procesos de verificación equivalentes, y antes de entrar en la concreción de lo que supone y debe suponer la realización de una auditoría RGPD, en este apartado presentamos los posibles usos que, las partes implicadas en la gestión de la protección de datos, pueden darles.

Así, desde un punto de vista de organizaciones que sean responsables de tratamiento, como hemos venido planteando, la realización de auditorías les permite:

- Evaluar los riesgos y verificar si las medidas son suficientes.
- Levantar nuevos riesgos.
- Adaptar nuevas medidas en un proceso de continua mejora.
- Demostrar cumplimiento.

Resultará, por tanto, muy recomendable que este aspecto -la realización de auditorías periódicas- quede contemplado y regulado en la gobernanza de la protección de datos de cada organización determinándose, en consecuencia, roles y responsabilidades respecto de la misma además de periodicidades (aspecto que abordamos en el siguiente apartado de esta Guía).

En relación con el regulador y la necesaria puesta a disposición de las auditorías al mismo, las conclusiones del informe, así como las medidas adoptadas, serán prueba del cumplimiento y, en su caso, de la proactividad de responsables y encargados del tratamiento.

Finalmente, en relación con los encargados del tratamiento -y como aspecto adicional al cumplimiento de la obligación que les impone el artículo 28 RGPD de colaboración con el responsable-, la realización de auditorías y la acreditación que las mismas puedan suponer sobre el cumplimiento de la normativa de protección de datos. Por su parte, se antoja un aspecto relevante -e incluso una ventaja competitiva- respecto de otros encargados que no dispongan de las mismas. Recordemos aquí la obligación que recae sobre los responsables de realizar una selección diligente de encargados del tratamiento.

3.4. Alcance

¿Qué es una auditoría en protección de datos o RGPD?

Conviene en este punto abordar y plantearse si el cambio en el contexto normativo ha supuesto también un cambio el concepto y alcance de las auditorías de protección de datos. Hasta la entrada en vigor del RGPD, las auditorías de protección de datos, tal como hemos señalado, estaban reguladas en el artículo 96 del RD 1720/2007. Dicho artículo no solo establecía los casos en los que resultaban obligatorias, sino que determinaba el alcance del informe, así como los roles y responsabilidades respecto de la misma y sus conclusiones.

Pues bien, ni en el RGPD ni en la LOPDGDD -como hemos venido exponiendo- se incluyen previsiones sobre estos aspectos. En consecuencia, en los siguientes apartados, analizaremos cuáles deberían ser las características y alcance de las auditorías de protección de datos al amparo del RGPD.

Concepto de Auditoría.

Existen multitud de definiciones de auditoría en función de su propósito (de cuentas, de certificación, de protección de datos…) así como en función de su naturaleza interna o externa. Así, por ejemplo, el Instituto de Auditores Internos define la auditoría interna como: *una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno*. Por su parte, la Asociación Americana de Contables se refiere a la misma como: *un proceso sistemático de obtener y evaluar evidencias de manera objetiva con respecto a afirmaciones sobre acciones y eventos económicos para determinar el grado de correspondencia entre las afirmaciones y el criterio establecido, y comunicar los resultados a los interesados*. En un ámbito más nacional, el Diccionario del español jurídico de la RAE y el Consejo General del Poder Judicial se refiere a la auditoría como: *la técnica profesional normada de revisión, verificación y evaluación de documentos contables y de procedimientos de control y de gestión cuyos resultados se recogen por escrito en un informe y contienen una opinión acerca de la información auditada, emitida con un grado de certeza medible estadísticamente.*

Podemos, en consecuencia, concluir que la auditoría es el proceso de aseguramiento

que, de forma independiente, trata de aportar una opinión objetiva acerca del nivel de control o exactitud del aspecto auditado con respecto a un criterio y permite determinar razonablemente el grado de confianza sobre dicho aspecto auditado.

Como características que deberá reunir una auditoría señalaríamos las siguientes:

1. **Independencia:** la libertad de condicionamientos que amenazan la capacidad del auditor para desempeñar sus responsabilidades de forma neutral.

2. **Objetividad:** es una actitud mental neutral, que permite a los auditores desempeñar su trabajo con confianza en el producto de su labor, y sin comprometer su calidad. La objetividad requiere que los auditores no subordinen su juicio al de otras personas en asuntos de su competencia y, asimismo, que no tengan conflictos de interés que condicionen su opinión.

3. **Efectividad:** cumple con los principios fundamentales para la práctica profesional de integridad, competencia y diligencia profesional; es objetiva y se encuentra libre de influencias (independiente); se alinea con las estrategias, los objetivos y los riesgos de la organización, está posicionada de forma apropiada y cuenta con los recursos apropiados, compromiso con la calidad y la mejora continua de su trabajo; se comunica de forma efectiva; proporciona aseguramiento en base a riesgos; hace análisis profundos, es proactiva y está orientada al futuro; y promueve la mejora de la organización.

En cuanto a los controles periódicos, ¿equivalen a una Auditoría?

Un control, de acuerdo con la definición del Instituto de auditores internos, es cualquier acción realizada para gestionar el riesgo e incrementar la posibilidad de cumplimiento de objetivos.

Según la UNE-ISO GUIA 73:2010: *los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen un riesgo*. Podemos diferenciar los controles por su carácter voluntario u obligatorio, por su ámbito de aplicación (administrativos, técnicos o físicos), por su función (preventivos, detectivos, correctivos), por su sistema de implantación (manuales o automáticos), o por los elementos a los que aplica.

Los controles periódicos son herramientas de las organizaciones para mitigar riesgos estableciendo unas pautas concretas a seguir mediante el análisis permanentemente

de las posibles desviaciones entre objetivos y realizaciones.

Como vemos, tanto la auditoría como los controles periódicos ayudan a la organización a cumplir con sus objetivos al aportar un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno. Sin embargo, no son equivalentes ya que mientras que los controles periódicos suponen una tarea regular integrada en los procesos de la compañía y su misión es la gestión del riesgo, la auditoría -por su carácter independiente- no puede estar ligada a los procesos operativos y su objetivo es la emisión de una opinión del grado de control con respecto a un criterio.

¿Qué aspectos debe evaluar una Auditoría RGPD?

Los principios de responsabilidad proactiva y el enfoque al riesgo comentados en los apartados anteriores, nos llevan a concluir que, a diferencia del régimen anterior, las auditorías a realizar bajo el RGPD deberán diseñarse y realizarse en función del tipo de organización que vaya a ser auditada, así como del momento, naturaleza o contexto de los tratamientos que la misma lleve a cabo.

En este contexto y sin perjuicio de que la planificación de cada auditoría deberá ir precedida de ese análisis previo, exponemos aquí los tres grandes bloques de aspectos que, en todo caso, deberían evaluarse (cuanto menos para decidir si es necesario o no incluirlos en el ámbito) y, en su caso, priorizarse.

a) Aspectos legales:

El RGPD recoge una serie de medidas cuyo incumplimiento podría conllevar la imposición de sanciones y ello sin necesidad de que exista una lesión previa de los derechos y libertades del interesado. Estas medidas, que denominaremos legales, son las siguientes:

- Tratar los datos personales conforme a las bases legitimadoras establecidas en el artículo 6 y, en su caso, 9 del RGPD.
- Cumplir con el deber de transparencia hacia el interesado en los términos de los artículo 12 y ss del RGPD.
- Gestionar los ejercicios de derechos de los interesados conforme los artículos 15 a 22 del RGPD.

- Incluir la protección de datos desde el diseño y por defecto, recogida en el artículo 25 en cualquier actividad que vaya a suponer el tratamiento de datos de carácter personal.

- Regularizar las relaciones de corresponsabilidad conforme lo establecido en el artículo 26 del RGPD.

- Regularizar las relaciones de encargo del tratamiento conforme el artículo 28 del RGPD.

- Disponer de un registro de las actividades de tratamiento, en los términos establecidos en el artículo 30, según el que se establece que, en determinados casos, el responsable y el encargado deberán llevar un registro de las actividades de tratamiento efectuadas.

- Implementar medidas que permitan la realización de una notificación de una violación de la seguridad de los datos personales a la autoridad de control y, en su caso, a los interesados, en los términos regulados en los artículos 33 y 34 del RGPD. Dentro de esta categoría resultará muy conveniente contar con procedimientos internos, normativa también de carácter interno, así como la realización de simulacros periódicos que permitan realizar un control efectivo.

- Realizar una evaluación de impacto en los casos previstos en el artículo 35 y, si fuera preciso, realizar la correspondiente consulta previa a la autoridad de control en los términos del artículo 36 del RGPD.

- En su caso, contar con un Delegado de Protección de Datos, como mínimo, en los supuestos contemplados en el artículo 37.

b) Aspectos organizativos:

Por riesgo organizativo entendemos aquel que afecte directamente a la propia estructura de la organización y a la toma de decisiones que garantice la reducción del riesgo de incumplimiento en la materia.

Unos mecanismos de gobierno que permitan tomar decisiones al nivel adecuado y con la información suficiente, y una estructura organizativa que permita la involucración/

participación de todas las áreas de una empresa en la protección del dato, determinarán el éxito en el grado de cumplimiento con RGPD.

Ahora bien, para ello será necesario comenzar con una correcta formación de todo el personal. La adopción de políticas y normas internas dirigidas a los empleados, colaboradores y proveedores, tanto con carácter general como focalizadas en relación a las funciones que desempeñen dentro de la empresa, jugará un papel decisivo en este objetivo.

Algunos ejemplos de políticas o de normas internas podrían ser:

- Políticas corporativas de protección de datos.
- Políticas de gobierno de la privacidad.
- Marco de controles en materia de protección de datos.
- Política sobre el uso de herramientas corporativas, recursos compartidos, etc.
- Normas internas que contengan los principios y reglas aplicables a la contratación de proveedores.
- Política sobre dispositivos móviles y el uso del teletrabajo.

Un programa de formación periódico general para nuevas incorporaciones o personalizado en función de las tareas desarrolladas dentro de la compañía, impulsarán la concienciación en esta materia y, por consiguiente, la proactividad en el cumplimiento de la norma.

Se trata, en definitiva, de conseguir una cultura de protección del dato como parte de la propia cultura de la organización.

c) Aspectos técnicos o de seguridad

El RGPD si bien avanza medidas de carácter técnico que se pueden considerar apropiadas para el cumplimiento de la norma, no se pronuncia sobre aquellas que garantizan la protección y, por consiguiente, el cumplimiento de la norma.

Así, las medidas que se señalan en el texto normativo son aquellas que permitan garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento en los términos del artículo 32 de RGPD.

En cualquier caso y de conformidad con el principio de *accountability*, serán las organizaciones las que decidan en cada momento, según el contexto y las actividades de

tratamiento llevadas a cabo por la misma, la oportunidad y bondad de las medidas técnicas a implementar.

Algunos ejemplos de medidas técnicas:

- Controles tecnológicos para la seguridad de la información.
- Medidas para la continuidad de negocio y recuperación ante desastres.
- Medidas para proteger el uso de herramientas habituales (correo electrónico) como antispam o antiphishing.
- Protección de Sitios Web.
- Realización de copias de seguridad y actualización de sistemas operativos.
- Cifrado de ficheros.
- Cifrado de discos.
- Sistemas de control de accesos.
- Cortafuegos.
- Herramientas que permiten analizar y controlar la actividad del usuario en el envío de información al exterior desde su puesto de trabajo mediante la detección de fugas de información.
- Gestión centralizada de contraseñas, control de accesos y sesiones: quién accede, cuándo y a qué.
- Gestión de usuarios.
- Políticas de respuesta ante incidencias y gestión de brechas de seguridad.

3.5. Enfoque

Analizados los aspectos que podría abarcar una auditoría, nos corresponde ahora analizar el enfoque y la periodicidad de la misma o, en otras palabras, diseñar cómo abordamos en una entidad u organización concreta la realización de una auditoría de cumplimiento de la normativa de protección de datos.

Tal y como se concluía en el apartado anterior, y teniendo en cuenta los principios de responsabilidad proactiva y enfoque a riesgos, a la hora de abordar una auditoría de una organización en concreto, habrá que tener en cuenta múltiples factores que determinarán su enfoque, diseño y periodicidad.

Uno de los primeros factores a tener en cuenta es el tamaño de la empresa. Así, por ejemplo, tendrá sentido hacer un enfoque completo (que aborde todos los aspectos señalados en el apartado anterior) para aquellas empresas pequeñas o medianas. Por el contrario, en el caso de grandes empresas, se podría plantear -cuando no resulte posible abordar ese enfoque completo- la adopción de un plan de auditorías que, por ejemplo, disgregue el gobierno y la gestión de la privacidad, por un lado, y la revisión de tratamientos, por el otro.

Otros factores que nos pueden determinar el enfoque de la auditoría a realizar podría ser el sector de la organización a auditar, existiendo, por ejemplo, sectores altamente regulados que ya prevén auditorías en otros ámbitos y que pueden resultar complementarias a la auditoría en protección de datos (tales como auditorías de seguridad).

La tipología de tratamientos realizados (por ejemplo, categorías de datos utilizados, existencia de transferencias internacionales de datos o la base de legitimación de los mismos) también pueden ser uno de los factores a tener en cuenta tanto para determinar el enfoque de la auditoría, su planificación o periodicidad. Así, por ejemplo, siguiendo criterios de escalabilidad podría abordarse la auditoría de los tratamientos atendiendo al criterio de prioridad de riesgo de los mismos continuando solo después con el resto, con el objetivo de finalizar con el 100% del registro de tratamiento de la organización auditado.

3.6. Periodicidad

Como se ha comentado anteriormente, la necesidad de revisar que se han implementado las medidas adecuadas y, además, de poder demostrarlo, está claramente identificada tanto en el RGPD, como en la LOPDGDD.

Ahora bien, como sucede con todos los aspectos de la nueva auditoría, tampoco queda claro, en ningún texto legal, la periodicidad con la que se debe realizar. Esto puede verse como una gran oportunidad para las empresas (aumentando el poder de decisión de las mismas) o como un vector adicional de riesgo, en el sentido de que disminuye la seguridad jurídica de la que se revestía la antigua LOPD y su Reglamento de desarrollo.

Si bien la empresa cuenta con el apoyo omnipresente del DPD, esto no resta para que la decisión final y el riesgo asociado pese sobre la compañía. Bajo el paraguas del principio de *accountability*, tanto el responsable como el encargado soportan la carga de dicha obligación. Y es precisamente sobre la base de *accountability* y proactividad que la em-

presa debe evaluar y redefinir su propio procedimiento de auditoría.

Con el fin de valorar la periodicidad, las empresas deben tener en consideración los siguientes criterios de variabilidad:

- **Riesgo:** los tratamientos de mayor riesgo, afectados por las Evaluaciones de Impacto relativas a la protección de datos (EIPD o PIA, por sus siglas en inglés) o de especial relevancia para el negocio (activos esenciales, afectados por ICFR, etc.) se posicionarían en primera línea de auditoría. Por tanto, su revisión requiere mayor frecuencia, que aquellos tratamientos de riesgo/relevancia medio o incluso leve.

  Dentro del criterio de riesgo, no hay que olvidar el relativo a las posibles sanciones en que se podría incurrir en caso de violación normativa. En este sentido, un estudio exhaustivo de la jurisprudencia, junto con un buen análisis de riesgos ayudaría.

- **Procesos:** en algunas empresas, se podría valorar la segregación de la auditoría según los distintos procesos de la empresa y así, la revisión más organizativa del Gobierno y Privacidad, dada su naturaleza más estática, requeriría una periodicidad inferior a la que podría necesitar el propio registro de tratamientos que se actualiza permanentemente.

- **Controles existentes:** una variable muy relevante a la hora de establecer una periodicidad de auditoría sería la preexistencia de controles periódicos en las empresas. Ya sea por exigencia interna de la compañía, o por la aplicación de normativas internacionales o nacionales, las empresas han podido desarrollar sistemas de controles internos que proporcionan aseguramiento continuo sobre diferentes ámbitos y que pueden ayudar a reducir el alcance de las auditorías.

No hay que olvidar que, con las antiguas normativas europeas, la auditoría, como concepto, no es desconocida y ya existen precedentes que pueden orientar a las empresas. De igual forma, el resto de normativa que afecta a las empresas de los distintos sectores[2] establecen todas obligaciones de auditoría en sus respectivos ámbitos de aplicación.

Por tanto, ya sea en base a nuestras antiguas referencias legales en materia de protección de datos, las últimas guías de las entidades competentes europeas o las actuales normativas de otros sectores aplicables, es aconsejable planificar auditorías específicas con enfoques y alcances coordinados que permitan obtener una visión completa de la situación de la compañía de forma cíclica.

[2] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información; Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, etc.

Esto, sin embargo, es simplemente orientativo, ya que lo que ahora corresponde a las empresas es valorar su situación actual y reajustar (si corresponde) su umbral de riesgo aceptable.

3.7. Auditoría Interna vs. Auditoría Externa

Tal como venimos comentando -y a diferencia de la normativa anterior-, ni el RGPD ni la LOPDGDD establecen mención alguna sobre las características de las auditorías y, por tanto, será responsabilidad también de las organizaciones decidir, para el caso que las realicen, si lo harán a través de auditorías internas, externas o se apoyarán en ambos tipos de auditores.

Auditoría interna y externa no deben entenderse, en ningún caso, como opuestas entre sí. De hecho, la principal diferencia que deberíamos encontrar entre ambas es la relación laboral o mercantil de los auditores en relación con la organización auditada.

En cuanto a los trabajos realizados por ambas -ante un mismo alcance- deberían ser similares, ya que las técnicas utilizadas en ambos casos son las mismas. Ambas centran su atención en aspectos de control interno y en la evaluación de riesgos para formular observaciones que, junto con una opinión general, quedan reflejadas en un informe de auditoría.

Sin embargo, sí que existen factores que pueden influir a la hora de decidir si realizar la auditoría de forma interna o externa, como pudieran ser, a título meramente ejemplificativo:

- La disponibilidad de recursos internos con el perfil y experiencia adecuados.
- Aspectos presupuestarios.
- La posibilidad de incluir el RGPD en los ciclos de planificación de auditoría interna.
- Potenciales conflictos de interés.

04

El proceso de Auditoría y las claves de su gestión

isms forum

4.1. Plan de Auditoría

Una de las funciones claves del gobierno corporativo en todos los sectores es la función de auditoría. El gobierno de la privacidad de los datos personales forma parte de dicho gobierno corporativo.

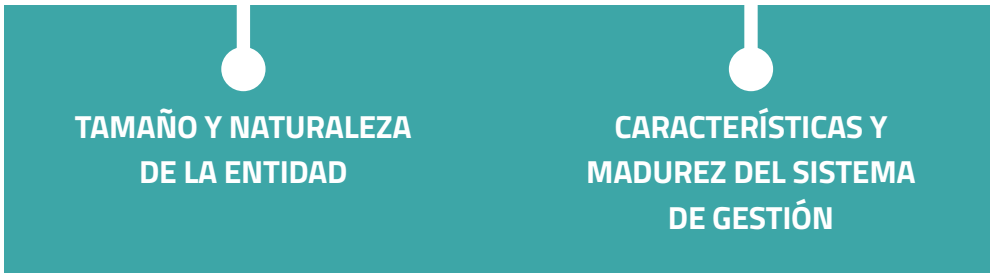
Como ya se ha tratado previamente, las empresas cuyos tratamientos de datos personales están sujetos a los requisitos del RGPD deberían realizar de forma periódica auditorías de cumplimiento del mismo para evaluar su nivel de cumplimiento. Dichas auditorías, propuestas normalmente desde las áreas de auditoria interna del Responsable de Tratamiento (realizado por sus propios medios o a través de un tercero), constituyen la tercera línea de defensa.

El RGPD brinda una mayor capacidad de disposición de los interesados sobre sus datos personales y además fomenta la autoresponsabilidad y autogestión de las empresas, puntos que hacen que tenga más sentido diseñar y realizar los programas de auditoría de protección de datos.

En este sentido, las auditorías de protección de datos personales deben proporcionar una visión independiente sobre el nivel de adecuación de los responsables y encargados de tratamientos a la legislación y normativas relativas a la protección de los datos personales de los ciudadanos. Más en concreto, las auditorías sobre protección de datos personales deben evaluar los controles de riesgos sobre la protección de los datos personales definidos e implementados por las empresas relativos a la organización, procesos y tecnología.

En líneas generales, las entidades deberían establecer un programa de auditoría que trate una o más normas de sistemas de gestión u otros requisitos, realizadas por separado o en combinación. La extensión de un programa de auditoria debería basarse en el tamaño y la naturaleza de la entidad auditada, así como en la naturaleza, funcionalidad, complejidad, el tipo de riesgos y oportunidades y el nivel de madurez de sistemas de gestión.

PROGRAMA DE AUDITORÍA

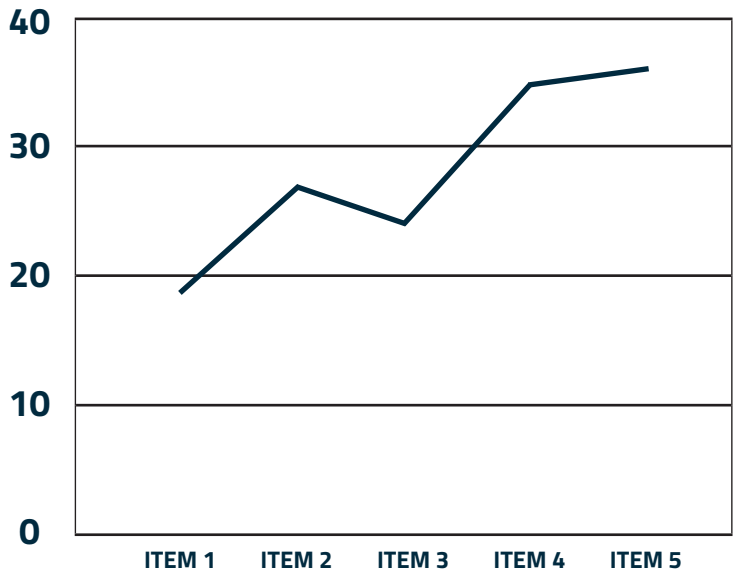


A la hora de diseñar un plan de auditoría se debería tener prefijado el o los objetivos que persigue, lo que permitirá orientar su planificación y ejecución, como por ejemplo los siguientes:

- **IDENTIFICACIÓN DE OPORTUNIDADES DE MEJORA** EN EL SISTEMA DE GOBIERNO DE LA PRIVACIDAD IMPLANTADO POR LA EMPRESA
- **EVALUACIÓN DE LA CAPACIDAD** DE LOS INTEGRANTES DEL GOBIERNO DE LA PRIVACIDAD PARA DESEMPEÑAR SU FUNCIÓN
- **IDONEIDAD DE LAS MEDIDAS** IMPLANTADAS
- **IDONEIDAD DEL ESQUEMA DE CONTROLES** IMPLANTADOS

La planificación de los programas de auditoría interna y, en algunos casos, los programas para auditar a los proveedores externos, pueden prepararse para contribuir a otros objetivos de la organización. Las personas responsables de la gestión del programa de auditoría deberían asegurarse de que se mantiene la integridad de la auditoría y de que no se ejerce una influencia indebida sobre la misma. Debería darse prioridad a la asignación de recursos y métodos para los asuntos de un sistema de gestión con los riesgos inherentes más altos y con los niveles de desempeño más bajos.

El programa de auditoría debería incluir la información e identificar los recursos que permitan que las auditorías se realicen de forma eficaz y eficiente dentro de los periodos de tiempo especificados. La implementación del programa de auditoría debería seguirse y medirse, de manera continua para asegurarse que se han alcanzado sus objetivos.



LO QUE NO SE MIDE NO SE PUEDE MEJORAR

4.2. Desarrollo del proceso de Auditoría y Dominios Funcionales

Conforme se ha expuesto en la presente Guía, podemos considerar que el proceso de revisión o auditoría debe ser un proceso que se debe realizar de forma periódica, y que debe englobar las medidas legales, técnicas y organizativas derivadas de la obligación de cumplimiento del RGPD y de la LOPDGDD, así como de otras políticas que pudiesen regular la actuación del responsable o el encargado del tratamiento en materia de protección de datos personales.

En el desarrollo de la auditoría se recomienda considerar los siguientes dominios funcionales:

DOMINIOS FUNCIONALES

- GOBIERNO DE LA PRIVACIDAD
- DPD/DPD
- LICITUD Y TRANSPARENCIA
- GESTIÓN DE DERECHOS
- PRIVACIDAD POR DISEÑO
- REGISTRO DE ACTIVIDADES
- ANÁLISIS DE RIESGOS Y EIPD
- NOTIFICACIÓN DE BRECHAS
- MEDIDAS DE SEGURIDAD
- ACCOUNTABILITY Y FORMACIÓN
- ENCARGADOS DEL TRATAMIENTO
- TRANSFERENCIAS INTERNACIONALES
- CORRESPONSABILIDAD

GOBIERNO DE LA PRIVACIDAD

Cómo se gobierna la privacidad en la entidad, qué roles están involucrados, cuáles son los procedimientos que marca la organización respecto a la protección de datos personales. Se deben evaluar todas las evidencias vinculadas.

- Política de Privacidad.
- Definición de Roles y funciones de Privacidad.
- Nombramiento y difusión de los responsables de privacidad.
- Normativa Interna de Privacidad: Políticas de privacidad, procedimientos, protocolos, estándares, procesos, etc.
- Acciones de comunicación y publicación de las funciones de Privacidad, roles implicados en la organización, así como políticas y procedimientos vinculados a la protección de Datos Personales.
- Identificación de la Autoridad de Control Principal.
- Revisión de comunicaciones a la Autoridad de Control. Por ejemplo, inscripción del DPD.
- Revisión de inspecciones, sanciones, consultas a la Autoridad de Control, etc.
- Códigos de Conductas y/o Certificaciones.
- Normas Corporativas Vinculantes.

DELEGADOS DE PROTECCIÓN DE DATOS (DPD/DPD)

La formalización de esta figura y las funciones que realiza el DPD/DPD. Dependiendo del alcance de la auditoría definido, pueden ser contempladas también en el proceso de auditoría.

- Análisis de la necesidad de DPD/DPD y decisión tomada por la entidad.
- Acta de nombramiento de DPD/DPD si aplica.
- Organigrama de entidad, posición de DPD/DPD y nivel de reporte.
- Canales de comunicación internos y externos con el DPD.
- Nombramiento y difusión de los responsables de privacidad.
- Análisis de compatibilidad/incompatibilidad de funciones.
- Análisis de la cualificación y dimensionamiento de la oficina del DPD/DPD.
- Revisión de funciones:
  - Comunicación, relación con el responsable, encargado de tratamiento y empleados.
  - Supervisión del cumplimiento.
  - Concienciación y formación.
  - Asesoramiento en evaluaciones de impacto.
  - Cooperación con Autoridad de Control.
  - Punto de contacto con Autoridad de Control y consultas.

LICITUD Y TRANSPARENCIA

Se debe evaluar si todos los tratamientos son lícitos y la idoneidad de la base legitimadora utilizada.

- Licitud de los tratamientos (Art.6).
- Transparencia en la información facilitada de los tratamientos (Art.12-13-14).
- Argumentación/Análisis de los tratamientos basados en interés legítimo.
- Revisión de Consentimientos.
- Revisión de Contratos.
- Revisión de Cláusulas Informativas.
- *Footers* de privacidad en correos electrónicos.
- Política de privacidad en las webs.
- Políticas de privacidad en zonas de acceso.
- Consulta a sistemas de exclusión publicitaria.

GESTIÓN DE DERECHOS DE LOS INTERESADOS

Cómo se actúa ante el ejercicio de derechos; cuál es el procedimiento a seguir; quién interviene; quién debe contestar; contestación en tiempo y forma.

- Procedimiento de Gestión de Derechos.
- Sistemas de información de los derechos de los usuarios.
- Formularios de solicitud.
- Canales de comunicación.
- Roles que intervienen.
- Listado de ejercicios de derecho ejercitados y revisión de ejecución de procedimiento y respuestas.
- Revisión de su efectiva aplicación tanto en bases de datos estructuradas como no estructuradas.

PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

Se debe evaluar la posición de la compañía respecto a este principio. Cómo se ha orquestado el análisis de la privacidad desde el diseño.

- Procedimiento de Privacy By Design y Privacy By Default.
- Principios de minimización de datos.
- Política de conservación de datos.
- Listado de iniciativas y evaluación de privacidad desde el diseño: Evidencias de su seguimiento (Actas de reuniones con la participación del DPD, requerimientos, seguimiento, resolución de consultas...).
- Evaluar si existen requerimientos para poder ejercer el bloqueo y limitación de tratamiento de datos personales desde el diseño.

REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

Revisión del registro de actividades de tratamiento, completitud del mismo, adecuada y actualizada la descripción de los mismos.

- Revisión del registro de actividades de tratamiento; completitud del mismo, adecuada y actualizada descripción de los mismos.
- Cuestionarios de validación de las distintas áreas.
- Finalidad de los tratamientos.
- Programas de gestión utilizados.
- Revisión de plazos de conservación de la información con respecto a la política de conservación.
- Revisión de accesibilidad de los datos según corresponda al tratamiento en el ciclo del dato.

ANÁLISIS DE RIESGO Y EVALUACIÓN DE IMPACTO

Revisión del modelo de riesgos de privacidad a distintos niveles y de la operativa llevada a cabo en este sentido.

- Metodología de Análisis de Riesgos de datos personales.
- Procedimientos de Evaluación de Impacto en datos personales (Art.35).
- Modelo/Formalización de los PIA's.
- Realización de análisis de Riesgos de datos personales de la entidad.
- Revisión de los procesos de Evaluación Objetiva - Análisis de Riesgos de datos personales.
- Revisión de las evaluaciones de Impactos en datos personales existentes.
- Revisión de Consultas a Autoridades de Control.
- Valoración de las medidas legales, organizativas y técnicas aplicadas para reducir los riesgos inherentes a los tratamientos.

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE DATOS PERSONALES

Revisión del modelo establecido para actuar ante brechas de seguridad y efectividad operativa del mismo.

- Procedimiento de Violaciones de Seguridad de Datos Personales.
- Evaluación del impacto de las brechas.
- Difusión del procedimiento de Brechas de Protección de Datos en la entidad y con los encargados de tratamiento de datos.
- Listados de brechas y análisis de impacto vinculado a las mismas.
- Revisión de los procesos de resolución/investigación de las brechas.
- Revisión de notificaciones de brechas realizadas ante la Autoridad de Control (Art.33). y afectados (Art.34).

MEDIDAS DE SEGURIDAD

La revisión de las medidas de seguridad vinculadas a los tratamientos de datos personales contempla todo su ciclo: la parte de establecimiento de las mismas en el momento inicial de diseño de la iniciativa (Privacy By Design) y las que derivan del análisis de riesgos y, en su caso, PIA, la aplicación de las mismas en los tratamientos que deben recogerse en el RAT (Artículo 30-RGPD) y revisar su correcto funcionamiento, así como actualización en caso necesario.

- Relación de medidas técnicas y organizativas vinculadas a los análisis de riesgo (PIA).
- Evaluar su adecuada implantación.
- Las medidas pueden ser de distinto tipo y naturaleza. Se recomienda ver la relación de medidas vinculadas a riesgo que se ejemplifica en el Anexo VI: Catálogo de amenazas y posibles soluciones de la *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD* de la AEPD.
- Algunas de las medidas técnicas más frecuentes implantadas para incrementar la integridad, disponibilidad, confidencialidad y resiliencia de la información personal son:
  - Sistemas de autenticación de seguros basados, en doble factor: token de un solo uso, biométricos, etc.
  - Cifrado de la información.
  - Pseudoanonimización que dificulte la identificación de los interesados.
  - Sistemas de alta disponibilidad.

ACCOUNTABILITY Y FORMACIÓN

Responsable del cumplimiento y deberá ser capaz de demostrarlo.

- Mantenimiento de los registros necesarios (derechos interesados, incidencias, accesos, etc.).
- Controles periódicos de cumplimiento en materia de protección de datos.
- Plan de formación y concienciación en materia de protección de datos.
- Evaluación de completitud, idoneidad de contenidos de protección datos.
- Se podría valorar entre las iniciativas de formación desarrolladas: el tipo de formación realizada (general, especializada por departamentos, etc.): periodicidad de la misma (semestral, anual): audiencias contempladas (identificación figuras críticas, ET, RT); ámbito territorial (centralizada, distribuida, formación de formadores).
- Acreditación de la formación realizada y de la asistencia a la misma.
- Valoración de indicadores.

ENCARGADOS DEL TRATAMIENTO

Persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable de tratamiento.

- Procedimiento de verificación del cumplimiento por los encargados de tratamiento de sus obligaciones.
- Análisis de idoneidad Encargados de Tratamiento.
- Cuestionario/evaluación de privacidad.
- Planificación de revisiones de Encargados de Tratamiento.
- Modelos de Contrato de Encargos de Tratamiento con acceso a datos personales.
- Adhesiones a Certificaciones o Códigos de Conductas.

TRANSFERENCIAS INTERNACIONALES

Flujo de datos personales desde el territorio del Espacio Económico Europeo, EEE (los países de la Unión Europea más Liechtenstein, Islandia y Noruega) a destinatarios establecidos en países fuera del EEE.

- Identificación de trasferencias internacionales.
- Confirmación de destinos con nivel de protección adecuada o transferencias mediante garantías adecuadas (Art.46): Normas Corporativas Vinculantes (Art.47), cláusulas tipo de protección de datos adoptadas por comisión (Art.93), código de conducta (Art.40) o certificación (Art.42).
- Gestión de peticiones a la Autoridad de Control.

CORRESPONSABILIDAD (ARTÍCULO 26)

Los escenarios de corresponsabilidad se detallan en el Reglamento General de Protección de Datos y se está incrementando en número de tratamientos en los que se adopta esta relación entre responsables que determinan conjuntamente los objetivos y los medios del tratamiento.

- Revisión de los acuerdos de corresponsabilidad de tratamientos.
- Revisión punto de contacto de los interesados del tratamiento.
- Revisión de coordinación entre los corresponsables para cumplimiento de obligaciones frente a los interesados.
- Revisión de cómo se aborda el deber de información (Art.13 y 14).

Sin perjuicio de las tareas detalladas en los apartados anteriores respecto de cada uno de los bloques funcionales, la revisión del grado de cumplimiento puede apoyarse asimismo en los estándares de privacidad o seguridad de la información, internacionalmente reconocidos a fin de garantizar que la auditoría comprenda la revisión de todos aquellos aspectos requeridos por la normativa aplicable.

En este sentido, a continuación se expone una relación de los bloques funcionales objeto de auditoría y los controles aplicables de los estándares internacionalmente reconocidos para la implementación de sistemas de gestión de la protección de datos:

- **Licitud de los tratamientos y transparencia:** ISO/IEC 27701:2019 – Anexo A – controles A.7.2.1 – A. 7.2.4., A.7.3.3, A.7.3.4.
- **Gestión de Derechos:** ISO/IEC 27701:2019 – Anexo A – controles A.7.3.1. – A.7.3.10.
- **Privacidad desde el Diseño y por Defecto:** ISO/IEC 27701:2019 – Anexo A – controles A.7.4.1. – A.7.4.9.

- **Registro de Actividades de Tratamiento:** ISO/IEC 27701:2019 – Anexo A – control A.7.2.8.
- **Evaluación de Impacto:** ISO/IEC 27701:2019 – Anexo A – control A.7.2.5.
- **Notificación de Brechas de Seguridad:** ISO/IEC 27701:2019 – apartado 6.13.
- **Medidas de Seguridad:** catálogo de controles de UNE-EN ISO/IEC 27002:2017.
- **Accountability:** ISO/IEC 27701:2019 – Anexo A – controles A.7.2.8, A.7.3.1.
- **Encargados de Tratamiento:** ISO/IEC 27701:2019 – Anexo A – controles A.7.2.6, 7.5.4.
- **Transferencias Internaciones (Artículo 44):** ISO/IEC 27701:2019 – Anexo A – controles A.7.5.1 – A.7.5.4.
- **Corresponsabilidad (Artículo 26):** ISO/IEC 27701:2019 – Anexo A – controles A.7.2.7,

Sin perjuicio de lo expuesto, si además de los tratamientos realizados en el rol de responsable del tratamiento, la entidad auditada pretende incorporar en el alcance de la auditoría los tratamientos de datos que realiza en calidad de encargado del tratamiento, habrán de contemplarse los siguientes dominios funcionales:

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

La revisión del registro de actividades de tratamiento que se realizan por cuenta de los responsables de tratamiento.

SUBENCARGADOS DEL TRATAMIENTO

La revisión de las medidas implementadas para garantizar que los subencargados otorgan garantías subicientes respecto al tratamiento de datos que realizan, así como la firma de los acuerdos subencargo con dichos terceros.

TRANSFERENCIAS INTERNACIONALES

La revisión de la regularización de transferencias internacionales a los subencargados ubicadas en países fuera del Espacio Económico Europeo.

MEDIDAS DE SEGURIDAD

La revisión de las medidas de seguridad vinculadas a los tratamientos de datos personales según las instrucciones del responsable del tratamiento y las implementadas por defecto por el encargado.

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE LOS DATOS

La revisión del modelo establecido para actuar ante brechas de seguridad y efectividad operativa del mismo, en particular, la obligación de notificar las brechas al responsable del tratamiento.

OBLIGACIONES CONTRACTUALES

La revisión de cumplimiento de las obligaciones establecidas en el artículo 28 del RGPD.

4.3. Las claves para la gestión de la Auditoría RGPD

Conforme a lo establecido en la Norma ISO 19001 de Auditorías de Sistemas de Gestión, podemos distinguir las siguientes fases fundamentales en el proceso de auditoría:

1. **Inicio** de la auditoría.
2. **Preparación** de las actividades de la auditoría.
3. **Realización** de la auditoría.
4. **Informe:** Preparación y distribución del informe de auditoría.
5. **Finalización** de la auditoría.
6. **Seguimiento:** Realización de actividades de seguimiento.

4.3.1. Inicio de la auditoría

El inicio de la auditoría se considera una de las fases más importantes del proceso. Consiste básicamente en la organización del proceso de auditoría y conlleva, entre otras, las siguientes actividades:

- Designar al líder del equipo auditor, al resto del equipo y a los expertos técnicos necesarios para la auditoría, los cuales, en todo caso, han de reunir las competencias requeridas.
- Elaborar un calendario de trabajo conforme a las necesidades de la auditoría.
- Establecer el plan de comunicación y el contacto inicial con el auditado.
- Definir los objetivos, el alcance y los criterios de auditoría.
  El objetivo puede ser certificar un sistema de gestión, hacer una auditoría global o valorar el estado de implantación en un departamento concreto.
- Seleccionar y determinar los métodos de la auditoría para llevarla a cabo de forma eficaz y eficiente, conforme a los objetivos, alcance y criterios definidos.
- Determinar la viabilidad de la auditoría, es decir, verificar que se tienen los recursos económicos y humanos necesarios para realizar la auditoría de forma efectiva.
- Valorar los riesgos. Es importante tener en cuenta los diferentes riesgos en relación al auditado.

4.3.2. Preparación de las actividades de la Auditoría

La segunda fase del proceso es la preparación de las actividades de auditoría, lo que supone:

- El análisis de la información documentada relevante del sistema de gestión del auditado.
- La planificación de la auditoría con un enfoque basado en el riesgo.
- Elaboración de un documento en el que se detallen las actividades, las personas involucradas y los días y horas en que se llevarán a cabo.
- El conocimiento del entorno, lo cual conlleva:
  - ✔ Conocimiento de las características específicas del sector económico en el que opere la compañía, incluyendo las guías de buenas prácticas referentes a la aplicación de la normativa de protección de datos que pudiese haber.
  - ✔ Características de la compañía: riesgos principales, controles establecidos, sector de actividad, cultura de cumplimiento etc.
  - ✔ El auditor debe contar con una perspectiva adecuada del negocio y del entorno.

- Análisis del organigrama de la compañía, del esquema y los roles que conforman el gobierno de privacidad en la misma.
- La auditoría debe dotarse de total independencia en la realización de su labor.

- La obtención de evidencias, incluyendo el estado de aplicación de las recomendaciones realizadas en las auditorías de protección de datos personales previas.

  La obtención de evidencias se realizará a través de la observación, medición, prueba o por otros medios, en todo caso habrá que tener presente que:

  - Las evidencias pueden ser extraídas tanto de forma directa (solicitud al área responsable) como indirecta (procesos de *mystery*).
  - Deben ser suficientes y adecuadas según el alcance de la auditoría.
  - Ha de garantizarse la independencia entre la fuente de la evidencia y la empresa.
  - Ha de comprobarse la inexistencia de contradicciones o, en caso de darse, analizar su porqué.

- Asignar las tareas de auditoría al equipo auditor. Además, es necesario preparar los documentos de trabajo.

4.3.3. Realización de la Auditoría

Durante una auditoría, se desarrollan una serie de actividades habituales como son:

- Realización de una reunión de apertura y asignación de trabajo, por el líder de la auditoría, al equipo de auditoría en las reuniones de equipo.

- Análisis y parametrización del nivel de cumplimiento:

  - Con el objetivo de identificar y concretar los aspectos más relevantes identificados en la auditoría. Los aspectos más relevantes serían los aspectos más significativos desde el punto de vista del nivel de cumplimiento de la normativa de protección de datos personales en su conjunto.
  - En esta fase se determinan las conformidades (cumplimientos), y no conformidades (no cumplimientos) respecto de los dominios funcionales propuestos en el presente capítulo. Las no conformidades deberían desarrollar recomendaciones mientras que las conformidades deben catalogarse en función del riesgo asociado.
  - Realización del diagnóstico respecto del cumplimiento.

- Determinación de conclusiones.

- Preparación de una reunión de clausura con el auditado.

Incluir o no alguna de esas actividades, el detalle y la formalidad con la que se lleven a cabo, variará según el tipo de auditoría, su alcance y la complejidad de la organización.

4.3.4. Preparación y distribución del Informe de Auditoría

La auditoría debe producir unos resultados y unas conclusiones que se plasman en un informe. Por ello, podemos diferenciar las siguientes fases:

- Preparación del Informe:
  - Realizar una comunicación clara de los aspectos más relevantes identificados en la auditoría. En el informe de auditoría podrán reflejarse en un apartado independiente.
  - Incluir todas las conformidades y no conformidades.
  - Relacionar de forma clara y concreta las recomendaciones derivadas del análisis realizado, justificando las mismas, asociándolas a las no conformidades.
  - El informe de auditoría debe componerse de un informe ejecutivo y un informe detallado, que recoja en detalle el trabajo realizado y las conclusiones.
  - El grado de cumplimiento de los criterios de la auditoría.
  - Las opiniones divergentes que, en su caso, puedan haber surgido.

- Distribución del Informe de Auditoria:
  - El Informe deberá emitirse dentro del tiempo acordado, motivándose los retrasos en caso de existir.
  - El borrador del Informe deberá facilitarse al responsable o encargado del tratamiento para su revisión.
  - Deberá distribuirse entre las partes interesadas pertinentes definidas en el plan de auditoria, garantizándose en todo caso la confidencialidad de su contenido.
  - Las recomendaciones del auditor deben facilitarse para su análisis al responsable o encargado del tratamiento. El resultado de cada recomendación podrá ser el siguiente:

    1. Podrá aceptarse, en cuyo caso el responsable o encargado del tratamiento tendría que indicar cómo y cuándo se llevaría a cabo la recomendación.

2. Podrá aceptarse con ajustes, indicando cómo y cuándo se llevaría a cabo la recomendación ajustada, en cuyo caso el auditor tendría que valorar los ajustes propuestos y dictaminar si acepta o no el ajuste.

3. Podrá rechazarse, en cuyo caso el responsable o encargado del tratamiento tendría que indicar los motivos por los que se rechaza. El auditor tendría que valorar las causas del rechace, y dictaminar si lo acepta o no.

4.3.5. Finalización de La Auditoria

- La auditoría se entenderá finalizada cuando se han llevado a cabo todas las actividades de auditoría planificadas, o según lo acordado con el responsable o el encargado del tratamiento.
- A su finalización, deberá conservarse o eliminarse toda la documentación relativa a la auditoría de acuerdo con lo establecido en el programa de auditoría.
- En el supuesto de existir necesidad por parte de los auditores de divulgación del contenido del Informe, deberán ser informados, lo antes posible, el responsable y el encargado del tratamiento.

4.3.6 Realización de Actividades de Seguimiento

- Auditar no termina con la presentación del Informe, sino que conduce generalmente a la implementación de acciones correctivas, por lo que es preciso realizar un seguimiento a los hallazgos y recomendaciones, sobre todo cuando se trata de hallazgos negativos.
- La empresa debe planificar las acciones correctoras derivadas de las recomendaciones aceptadas.
- Debe realizarse un seguimiento de la planificación de la adopción de las medidas correctoras.
- Según se vayan aplicando las acciones correctoras éstas deben documentarse.
- Las auditorías internas suelen realizarse para cumplir el requisito de un sistema de gestión. Así, el mismo sistema determina qué hallazgos de auditoría deben ser objeto de monitoreo y seguimiento.
- El resultado de las auditorías debe facilitar la toma posterior de decisiones en base a un conjunto de recomendaciones.

05

Conocimiento del entorno y obtención de evidencias

isms forum

5.1. Preparación de la Auditoría

La auditoría es un proceso sistemático, independiente y documentado mediante el cual se expresa una opinión objetiva sobre el nivel de cumplimiento de una entidad respecto de un determinado estándar. Habiendo establecido lo anterior, es indudable que el conocimiento de la empresa a auditar sea clave para la realización de una buena auditoría.

Los objetivos de la auditoría deben incluir los que enuncia la *Guía de Auditoría* del ENS:

> *Emitir una opinión independiente y objetiva, basada en los principios de integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia y enfoque basado en la evidencia, sobre este cumplimiento de tal forma que permita a los responsables correspondientes tomar las medidas oportunas para subsanar las deficiencias identificadas, si las hubiera, y atender a las observaciones que pudiera haber identificado el Equipo Auditor y, en su caso , posibilitar la obtención de la correspondiente Certificación de Conformidad. (...) El objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado; tanto internamente como frente a terceros, que pudieran estar relacionados.*

En la fase de preparación de auditoría, según las circunstancias, se debe iniciar el conocimiento de la compañía, o bien se debe profundizar en este, en caso de estar ya familiarizado con la misma o disponer de un conocimiento previo.

Así, es necesario conocer:

PREPARACIÓN DE LA AUDITORÍA

- A qué se dedica la compañía: para ello es relevante la información sobre su sector de actividad, las áreas de negocio de la compañía y principales clientes.
- Su dimisión y como se organiza.
- El grado de digitalización de su negocio.
- Las certificaciones relevantes a esta materia que tiene en vigor.
- Los datos de carácter personal que trata y con qué propósito.
- Si ha tenido alguna sanción.
- Si ha tenido algún incidente de ciberseguridad.

A esta lista, y en el caso de no ser la primera vez que la entidad es auditada, es relevante incluir el resultado de las auditorías anteriores.

Este conocimiento es necesario para establecer, en esta fase, como mínimo:

- El programa de auditoría, incluyendo el alcance y los objetivos, indicando los roles de las personas de la compañía que deberán atender las peticiones del equipo auditor,
- La propuesta del plan de la auditoría; debe ser detallada y calendarizada con el objeto de que puedan bloquearse los recursos internos y externos que deberán intervenir en cada uno de los ámbitos a auditar identificados en el plan,
- El equipo auditor, teniendo en cuenta la competencia de sus miembros en función de la compañía, el alcance (los tratamientos), sus socios y despliegue internacional[3] y su entorno tecnológico; debe garantizarse que el equipo auditor cuente con los conocimientos suficientes para asegurar la adecuada realización de la auditoría.

También en esta fase deberán firmarse los acuerdos necesarios para que el equipo auditor tenga acceso a las fuentes de evidencia necesarias para la realización de la auditoría. Estos acuerdos deben incluir, como mínimo, el acuerdo de confidencialidad y el de privacidad.

5.1.1. Información relevante

La información relevante comprende toda aquella que permite que el trabajo de auditoría cumpla los objetivos de la misma, es decir, determinar el grado de alineamiento de la entidad con respecto a los requisitos requeridos por el RGPD y la LOPDGDD, conforme

[3] La entidad puede estar sometida a requisitos adicionales debido a su despliegue internacional.

a la planificación establecida.

Iniciada la auditoría y, a lo largo de todas las etapas del trabajo, se pueden identificar diferentes tipos de información relevante:

- Conocimiento sobre el modelo de privacidad[4], incluyendo debilidades de control previas y acciones llevadas a cabo por la entidad para su subsanación.
- Conocimiento general acerca de entidad y sobre su modelo de privacidad:
  - Entidad interna, organigrama y dependencias.
  - Roles y responsabilidades en materia de privacidad: existencia de DPD, nivel de reporte, existencia de Comités de Privacidad.
  - Procesos de privacidad: gestión de RAT, gestión de derechos de los interesados, gestión de encargados del tratamiento, gestión de brechas de seguridad, gestión de transferencias internacionales de datos, etc.
  - Políticas, guías y procedimientos de privacidad, que constituyen el modelo de privacidad en la entidad.
    - Política de Privacidad, documento en el que se plasme la estrategia, objetivos o principios acerca de la privacidad en la entidad.
    - Política de Seguridad de la Información, documento en el que se plasmen las estrategias y medidas de seguridad adoptadas en los sistemas de información que traten los datos personales.
    - Guías y procedimientos, documentos que, de mayor a menor nivel de abstracción, formalizan las prácticas sobre los procesos de privacidad y seguridad de los datos.
- Información relativa a la planificación, planes de trabajo y guías de auditoría conforme a la información de control interno de la entidad.
  - Planificación que cubra todos los objetivos de la auditoría.
  - Planes de trabajo que desarrollan cómo se van a abordar los artículos a analizar.
  - Planes de entrevistas y reuniones a mantener dentro de la entidad.
  - Guías de auditoría, herramientas, ya sean automatizadas o plantillas de trabajo, que den soporte al análisis de procesos y sistemas que den soporte a los tratamientos objeto de análisis.
- Información relativa a otras auditorías y revisiones realizadas por la propia entidad:

[4] Modelo de privacidad es equivalente al Modelo de Control Interno que tiene una entidad, pero aplicado a la gestión de la privacidad y al cumplimiento de los requerimientos del Reglamento.

- Mediante recursos propios (Auditoría Interna o Control Interno).
- Por parte de terceros independientes.

- Evidencias de auditoría obtenidas dentro del análisis preliminar y del propio trabajo de campo de la auditoría de protección de datos personales.

  Buena parte de la información relevante recogida conformará las evidencias de auditoría que el equipo auditor deberá presentar para soportar sus conclusiones y afirmaciones, así como para la elaboración de recomendaciones para solventar las potenciales deficiencias que se detecten.

  Aunque la información relevante se recoge durante todo el proceso de auditoría, típicamente, se obtendrá en las fases descritas en los siguientes epígrafes.

5.1.2 Análisis preliminar

Esta etapa, que forma parte del proceso de auditoría, tiene lugar antes de que el equipo auditor realice el trabajo dentro de las instalaciones de la entidad. Las evidencias para este análisis preliminar habitualmente se obtienen de:

EVIDENCIAS PARA EL ANÁLISIS PRELIMINAR

ENTREVISTA CON LA DIRECCIÓN DE LA ENTIDAD

Para el conocimiento del ambiente de control. Es recomendable que asista el espónsor de la auditoría, la gerencia del equipo auditor y el DPD, en caso de haber sido definido.

AUDITORÍA DOCUMENTAL

De forma análoga a procesos de certificación como las normas ISO auditadas bajo la guía, *ISO 19011:2018 Guidelines for auditing management systems*, se realiza una petición anticipada de información relevante que soporte el modelo de privacidad de la entidad.

A partir de las mismas, se obtendrá al menos la siguiente información relevante:

- Las Políticas, Guías y Procedimientos de Privacidad, Seguridad de la Información, Organigramas, organización interna y el RAT.
- La identificación de los interlocutores, áreas a revisar, procesos, sistemas, aplicaciones y encargados del tratamiento.

5.1.3. Trabajo de campo

En esta etapa se llevan a cabo las entrevistas, muestreos y análisis de evidencias que soportan el modelo de privacidad y los procesos que lo implementan. Se obtendrán:

- Hallazgos: hechos relevantes con respecto al trabajo de auditoría que, una vez contrastados debidamente, pueden convertirse en evidencias de auditoría.
- Elementos que, con independencia de su naturaleza y forma de obtención, soporten las afirmaciones del auditor al respecto de no conformidades y observaciones.

5.1.4. Diferentes métodos de obtención de evidencias

Según la R.A.E., una evidencia es una certeza clara y manifiesta de la que no se puede dudar y, como segunda acepción, quizá más precisa en este contexto, es la "prueba determinante en un proceso".

En el entorno de auditoría, esto implica que las evidencias deben ser suficientes y adecuadas, de forma que permitan alcanzar conclusiones razonables en las que el auditor podrá basar su opinión.

Cómo obtener esas pruebas (suficientes y adecuadas) que garanticen la certeza de cumplimiento:

a) Definición de las pruebas

Para ello se deberá tener en cuenta qué se pretende probar. No es lo mismo probar -o comprobar- el cumplimiento de una norma, que la consistencia de los controles ya existentes o el sistema de gestión implantado.

También deberá tenerse en consideración la naturaleza del auditado, el conocimiento

del entorno y, por supuesto, el riesgo sobre el activo a auditar.

Por ejemplo, en entornos en la Nube, eminentemente tecnológicos o automatizados, la definición de las pruebas de comprobación de la seguridad tenderá más a aspectos técnicos que físicos, sin embargo, en entornos con mayor existencia de archivos físicos, cámaras de vigilancia, controles de accesos, etc. será más fácil encontrar evidencias físicas o mediante técnicas de observación.

Por último, no debe perderse de vista que la evidencia debe ser suficiente (cuantitativamente) y adecuada (cualitativamente), pero manteniendo una proporcionalidad; la auditoría no debe impedir que la auditada siga en funcionamiento y desarrolle su actividad con normalidad.

b) Selección de elementos sobre los que practicar las pruebas

Se puede empezar consultando a la propia entidad qué controles tiene instaurados, con ello ya conoceremos la existencia o inexistencia de controles, la eficacia o ineficacia de los mismos y en definitiva si existe un entorno de control adecuado. A falta de claridad o concreción por parte de la auditada, será muy útil comenzar por una aproximación basada en el riesgo del activo a auditar. La selección de elementos sobre los que realizar pruebas podrá cubrir el 100% de los elementos si la muestra es pequeña o resulta crítica en un enfoque basado en el riesgo o, en su defecto, en una selección de los elementos considerados clave o más críticos en términos de riesgo o, por último, simplemente una muestra significativa en porcentaje en el caso de poblaciones muy numerosas (muestreo).

5.1.5. Procedimientos para obtener la evidencia de Auditoría

1 Inspección

Podemos distinguir aquí dos tipos de inspección: física y documental. En la inspección física, y dependiendo del riesgo de la entidad auditada, se podrá obtener información muy valiosa de cara al cumplimiento RGPD con una visita a las instalaciones donde se ejerza la actividad, por ejemplo: cartelería (videovigilancia), información de interés, formularios de contacto o tablón de anuncios. Además, se podrá comprobar la seguridad física y lógica en los accesos físicos y posibles, actividades de tratamiento (llaves, biométrica, tarjetas de acceso, registros de entrada, murallas físicas o lógicas en archivos documentales o servidores…).

La inspección documental facilitará además información sobre procedimientos internos, procesos, registros, activos, PIA, etc. y será determinante a la hora de valorar cualitativamente el grado de cumplimiento de la entidad. En la inspección documental se deberá valorar los elementos sobre los que realizar las pruebas (muestreo).

2 Observación

Consiste en presenciar un proceso o procedimiento. Con ello se puede obtener evidencia del grado de conocimiento de los empleados de los procedimientos internos, del ciclo de vida del producto o servicio, del entorno y actividades de control, etc. Con este método se podrán obtener evidencias de gran valor, por ejemplo, en cuanto a firma de cláusulas de protección de datos en contratación presencial o a distancia, o ejercicio de derechos.

Aunque tradicionalmente la planificación de la auditoría requiere del conocimiento de la auditada sobre las pruebas a realizar, poco a poco se van imponiendo en el mercado técnicas de *mystery shopper*, en las que se realiza una comprobación anónima simulando ser un cliente. Estas técnicas pueden resultar adecuadas en una auditoría como apoyo para conocimiento de un proceso de aceptación de clientes (*on boarding*) o de ciclo de vida del cliente de principio a fin (*end-to-end*).

3 Procedimiento analítico

En el ámbito del cumplimiento RGPD, este método puede resultar muy útil para comprobar una adecuada gestión del riesgo, y podría basarse en comprobar la sustentación metodológica de la identificación y escenarios de riesgo, a los efectos de valorar si la entidad ha aprobado sus políticas de privacidad y seguridad desde el diseño y por de-

fecto, así como la metodología para la realización de evaluaciones de impacto. Tanto las guías de la AEPD como las herramientas "Informa", "Facilita" y "Gestiona" pueden ser de gran ayuda para esta valoración.

4 Confirmación externa

Sería la comprobación por parte de un tercero del cumplimiento de la auditada. Se puede realizar respecto de proveedores o clientes, dentro de entrevistas o incluso por escrito. En el ámbito RGPD y de la seguridad puede cobrar relevancia en la relación (muchas veces diluida en cuanto a responsabilidades y tareas) entre responsables, corresponsables y encargados, así como en los casos de brechas de seguridad, realización de pruebas de seguridad o continuidad de negocio.

5 Indagación (entrevistas)

Es la obtención de información por parte de personas bien informadas o involucradas dentro de la auditada. Este procedimiento puede servir de apoyo a la hora de corroborar incongruencias detectadas por medio de otras evidencias, físicas o documentales, así como para comprobar el grado de concienciación o conocimiento dentro de la auditada. Dependiendo del riesgo, podría ser necesario requerir prueba escrita de esa indagación o incluso requerirse la suscripción de declaraciones de control o cuestionarios de cumplimiento para los Directivos o puestos clave en la entidad.

6 Utilización de otras fuentes, el trabajo de terceros y externos, o auditorías anteriores

Se puede obtener información valiosa y relevante a través de controles de calidad de los procesos, el trabajo realizado por auditorías anteriores o incluso por auditorías realizadas por otros terceros. Es aquí donde resulta esencial valorar la calidad y objetividad

del trabajo realizado por el tercero. Por ejemplo, si se utiliza un informe de control interno sobre calidad de procesos, será más valioso si la entidad ha obtenido una certificación de calidad del proceso que nos garantice que ese control interno se ha realizado con un determinado estándar que simplemente obtener un control interno al uso, que aun siendo adecuado como evidencia, podría no ser suficiente por sí solo como para considerarlo evidencia del control (de hecho la adhesión a un código de conducta o la obtención de una certificación por un organismo autorizado puede ser considerado prueba del cumplimiento de la obligación prevista en el artículo 32 del RGPD -seguridad del tratamiento-).

En ocasiones estos informes, aunque valiosos, pueden solaparse con la auditoría de RGPD. Es el caso de las auditorías previstas en el 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 (ENS). Esta misma Guía prevé la posibilidad de utilizar un mismo equipo auditor o diferenciados, así como la emisión de dos informes o un único informe agrupado. La elección sobre la adecuación del tipo de informe, de nuevo, deberá evaluarse conforme a los criterios indicados anteriormente.

Durante la planificación y desarrollo de la auditoría deben tenerse en cuenta los diferentes tipos de evidencias que van a recopilarse y sus requisitos. Estos deberán garantizar en cada caso, que se alcance un nivel óptimo de fiabilidad o confiabilidad, dicho de otro modo, la evidencia debe probar el efectivo cumplimiento del requisito y/o medida de seguridad implementada.

- Las evidencias se podrán obtener a partir de la solicitud al área responsable, o mediante el análisis y observación de facto de los procesos, test de los sistemas informáticos o procesos de *mystery*.
- Debe garantizarse la independencia entre la fuente de la evidencia, y la empresa o el área concreta que se esté auditando. En este sentido, habrá que prestar especial atención a las evidencias proporcionadas por el área responsable auditada.
- Deberán ser, como ya se explicó, suficientes y adecuadas, teniendo en cuenta el alcance de la auditoría.
- Se deberá comprobar la inexistencia de contradicciones y, en tal caso, analizar la causa de las mismas.

Los diferentes tipos de evidencias a tener en cuenta serán:

- Observación de procesos y existencia de elementos físicos.
  - Monitorización de los sistemas de red y seguridad durante la operativa.
  - Inventario de los equipos multimedia, almacenamiento y localización de los mismos.
- Evidencias documentales, registradas en papel o digitales.
  - Políticas y procedimientos.
  - Resultados de consultas a bases de datos.
  - Registros y/o logs de operaciones (acceso, almacenamiento, edición, borrado).
  - Cualquier documentación relevante llevada a cabo de forma habitual durante el desarrollo del negocio.
- Declaraciones y respuestas del personal implicado a través de entrevistas.
- Resultado del análisis, comparativa o simulación de operativas.

5.1.6 Requisitos de las evidencias

Es necesario definir los requisitos de las mismas para garantizar que son suficientes y adecuadas teniendo en cuenta el alcance de la auditoría. Para ello, podemos dividir y organizar las evidencias en los dominios de cumplimiento detallados en el capítulo anterior de esta Guía. Sin perjuicio de lo indicado en los apartados anteriores, respecto a las características de las evidencias, es recomendable que las evidencias a solicitar se adecúen a las casuísticas particulares de cada dominico funcional.

06

Análisis y valoración del nivel de cumplimiento

isms forum

Una vez obtenidas las evidencias de cumplimiento del RGPD, sobre las que se apoyarán las conclusiones y recomendaciones del informe de auditoría, se deberá analizar y valorar el nivel de cumplimiento en base a las diferentes evidencias obtenidas que, con carácter general estarán sustentadas en datos, hechos y observaciones recogidos en la fase previa.

En síntesis, el informe de auditoría deberá dictaminar hasta qué punto las medidas o controles técnicos, jurídicos y organizativos dan una respuesta adecuada a los requisitos y exigencias de la regulación, identificando las deficiencias, y proponiendo nuevas medidas y controles correctivos.

El análisis y valoración del nivel de cumplimiento es uno de los puntos más controvertidos de la auditoría, puesto que el grado de cumplimiento o incumplimiento de una norma muchas veces depende de la interpretación subjetiva de quien la tiene que aplicar, frente a quien la tiene que auditar.

Para evitar este grado de subjetividad en cuanto al cumplimiento normativo, se deberán tener en consideración una serie de métricas o indicadores que serán las que nos permitan conocer si estamos correctamente situados en la zona de cumplimiento, o en la de incumplimiento y, sobre todo, se deberá valorar si la propia empresa tiene predefinidos estos indicadores, puesto que al final es lo que determina si el sistema de gestión del riesgo es adecuado o, en términos del RGPD, si se ha adoptado un enfoque basado en el riesgo.

6.1. Conceptos previos

Existen algunos conceptos clave que utilizaremos en esta parte de la guía respecto de la valoración del cumplimiento (basados, principalmente, en las definiciones contenidas en la *Guía CCN-STIC 815* del ENS sobre *Métricas e indicadores*[5] , así como la *Guía de auditoría CCN-STIC 802* del ENS[6]; aunque podrían utilizarse otros, como los incluidos en la familia ISO 27000, o en COBIT, del ISACA. A continuación, se definen esos conceptos a fin de facilitar la comprensión de esta parte de la guía:

- **Comprobación.** Dentro del contexto de esta Guía, son verificaciones de la realización de controles, del establecimiento de medidas de seguridad, y de documentación de políticas, entre otros, dentro de los requerimientos establecidos por la norma de referencia en la auditoría.

- **Control.** Mecanismo o procedimiento que evita, previene, o detecta un riesgo. Es referido a toda medida que ayuda al cumplimiento de los principios y obligaciones determinados por el RGPD, resto de normativa aplicable en protección de datos, así como derivados de estándares de cumplimiento de

[5] Guía CCN-STIC 815 del ENS sobre "Métricas e indicadores".
[6] Guía de auditoría" CCN-STIC 802 del ENS.

seguridad. En el contexto de una auditoría, los controles pueden ser clasificados en preventivos, de detección, y correctivos.

- **Cuadro de mando.** Conjunto de indicadores para resumir el estado de situación.

- **Evidencia de auditoría.** Registros, declaraciones de hechos o cualquier otra información que es pertinente para los hallazgos de auditoría y que es verificable. La evidencia de auditoría puede ser cualitativa o cuantitativa.

- **Indicador.** Representación de una métrica de manera sencilla e intuitiva (generalmente en %): % de tratamientos realizados en la compañía que incluyen categorías especiales de datos; % del nivel de riesgo de dichos tratamientos. Instrumento que se utiliza para monitorizar el objetivo o la meta preestablecida. Los más relevantes son los denominados clave (Key) que serán sobre los que habrá de prestarse una mayor atención. Los utilizados más comúnmente son los Indicadores clave de riesgo ("Key Risk Indicators", KRI por sus siglas en inglés) y los Indicadores clave de rendimiento o desarrollo ("Key Performance Indicators", KPI por sus siglas en inglés).

- **Madurez y eficacia.** Capacidad de lograr el efecto que se desea o se espera en el marco del cumplimiento de los requisitos exigidos por el RGPD, resto de normativa aplicable en protección de datos, así como derivados de estándares de cumplimiento de seguridad.

- **Medición.** Proceso consistente en la asignación de números o símbolos que nos permitan describir una entidad de acuerdo con unas reglas claramente definidas. También se puede entender como comparación de una cantidad con una unidad u objeto que se usa de referencia.

- **Medida.** El número o símbolo asignado a una entidad como resultado de un proceso de medición. La medida sirve para caracterizar un atributo de la entidad.

- **Métrica.** Unidad de medida del grado de consecución de una meta o un resultado esperado, que permita interpretar lo que ocurre, es decir, que tiene una finalidad, de forma que sirva de herramienta para entender la realidad y tomar decisiones al respecto. Las métricas deben ser:

  - Definibles: Basadas en datos objetivos.
  - Comprensibles y manejables: Tanto para el área auditada como para negocio.
  - Replicables: Que permitan contrastar su evolución a lo largo del tiempo.
  - Relevantes: Que proporcionen información veraz y útil.

- **Valor.** Asignaciones numéricas de cada variable según la relevancia cualitativa de determinados factores en la implementación efectiva de los controles.
- **Variable.** Determinada característica o circunstancia que permite, en cómputo global con el resto de las variables a tener en consideración, analizar la madurez y eficacia de los controles del cumplimiento mediante la asignación de valores numéricos.
- **Verificación.** Cualquiera de las acciones de auditoría encaminadas a la comprobación el cotejo, el contraste y el examen de evidencias, registros y documentos.

Con todos estos elementos ya definidos, y las evidencias recopiladas, se podrá configurar la valoración del cumplimiento.

La propia entidad auditada es la que hace normalmente el ejercicio de autoevaluación del grado de cumplimiento. Este aspecto resulta especialmente sensible, ya que una definición de metas u objetivos que cumpla sobradamente la legislación y que a la vez sea demasiado ambiciosa en plazos o porcentajes de error, podría provocar no alcanzar nunca el indicador de cumplimiento, lo que no significaría necesariamente que ese grado de incumplimiento tenga como consecuencia una sanción de la Autoridad de Control, y por el contrario, la definición de metas u objetivos menos exigentes en cuanto a porcentajes, plazos o cumplimiento de normas específicas podría determinar una autoevaluación plenamente satisfactoria que, sin embargo, de cara a la Autoridad de Control, podría ser objeto de una sanción.

Por ello, será fundamental adoptar alguna metodología o estándar que permita definir previamente, de forma más o menos estructurada, los indicadores que se utilizarán. La labor de la auditoría en este sentido deberá concluir si realmente se utilizan tales indicadores y si los mismos se han establecido utilizando una metodología propia o estandarizada.

6.2. Descripción del marco de valoración de cumplimiento

Una de las cuestiones a tener en cuenta son los elementos que se deberán valorar en la auditoría a la hora de hacer un juicio de valor sobre el cumplimiento del RGPD.

En este sentido, la AEPD, dentro de su catálogo de guías para facilitar el cumplimiento, publicó un listado de cumplimiento normativo[7] de mucha utilidad como *check list* (lista de verificación) o base de un cuadro de mando. Este listado recoge todos los elementos que, en un sistema de gestión de riesgos, la entidad auditada debe recopilar y permitirle evidenciar el cumplimiento. Ahora bien, debe tenerse en cuenta que el listado es una

[7] Listado de Cumplimiento Normativo de la AEPD.

referencia de ayuda, luego las especificaciones de cada compañía pueden aconsejar una aproximación distinta o incluso nuevos elementos para valorar los riesgos de incumplimiento.

Incluso debería valorarse si el nivel de detalle de la respuesta a ese listado permite conocer si existen métricas y evidencias adecuadas que respalden la respuesta o, si por el contrario, se precisa desarrollar un sistema de gestión de riesgos que respalde con más solvencia y precisión el grado de satisfacción con el cumplimiento del apartado concreto de la norma objeto de auditoria, puesto que contestar a este cuestionario con un simple "si/no", sin evidencias que respalden el grado o porcentaje de cumplimiento, impediría acreditar realmente el cumplimiento de la norma.

A este respecto, podemos acudir a las instrucciones de la UNE-EN ISO 19011:2018[8] de *Directrices para la auditoría de los sistemas de gestión*, que indica (Anexo A, respecto de las auditorias de cumplimiento) que se deberá valorar si el auditado dispone de procesos eficaces para:

- Identificar requisitos legales y reglamentarios que le sean de aplicación.
- Gestionar sus actividades, productos y servicios para lograr el cumplimiento de estos requisitos.
- Evaluar su estado de cumplimiento.

Y si junto con estos procesos, se dispone de:

1. Un proceso eficaz para identificar cambios normativos.
2. Personas competentes para gestionar sus procesos de cumplimiento.
3. Información apropiada sobre su estado de cumplimiento.
4. Programa de auditoría interna.
5. Trata todas las instancias de no cumplimiento.
6. Tiene en consideración el desempeño del cumplimiento en sus revisiones por la dirección.

En cualquier caso, dado que el cumplimiento del RGPD requiere de un enfoque basado en riesgos, la gestión de estos es un pilar fundamental a la hora de abordar dicho cumplimiento normativo, así como un elemento referente en la auditoría del mismo. Así, la aproximación se deberá llevar a cabo de una manera sistemática, interativa y colaborativa.

[8] "Directrices para la auditoría de los sistemas de gestión", (UNE-EN ISO 19011:2018).

Las fases principales serán las siguientes:

1. La fase de identificación tiene como objeto abordar el control (del cumplimiento) cuya efectividad ha de ser auditada, que podrá devenir tanto de la interpretación del RGPD como de cualquier estándar adoptado por la compañía, así como de lo contenido en la presente Guía.

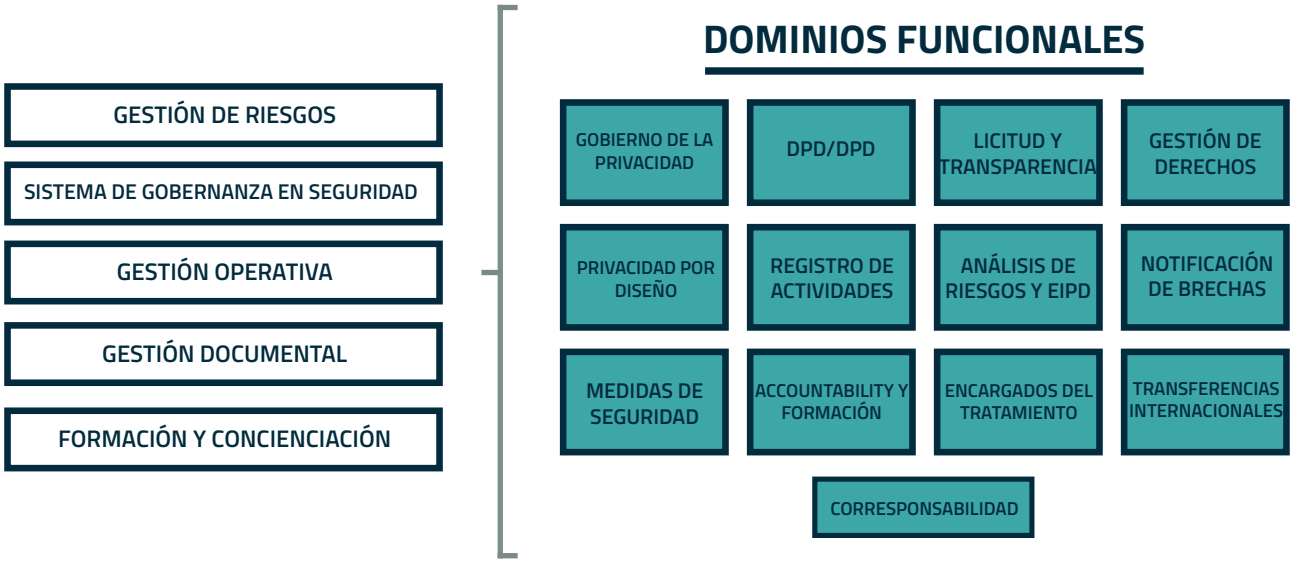
2. Por su parte, el análisis implica la consideración detallada de las variables de cada control, determinadas por las características y circunstancias de este.

3. Finalmente, la valoración se llevará a cabo mediante la asignación de un número indicativo de la relevancia de cada variable en el marco de la eficacia del control, resultando así una cuantificación objetiva del conjunto de controles del cumplimiento con los que cuenta la compañía, incluyendo su eficacia.

Por tanto, la culminación de estas fases permitirá la priorización de medidas enfocadas a garantizar la reducción o eliminación de los riesgos inherentes (o incluso residuales no corregidos adecuadamente) del tratamiento de datos personales. En este sentido, el propósito de la valoración de la eficacia de los controles es apoyar a la toma de decisiones en la compañía, de manera que, aunque no necesariamente determinen una actuación decidida por parte de ésta, redunden en el refuerzo del sistema de evidencias que, en cumplimiento del principio de responsabilidad proactiva, todo responsable o encargado del tratamiento ha de construir.

6.3. Principales métricas e indicadores en Auditorías de cumplimiento del RGPD

El resultado de toda auditoría se mide en función de los hallazgos encontrados que deben estar soportados en indicadores de cumplimiento. A continuación, se enumeran los cinco principales **dominios de gestión** de la privacidad bajo los cuales se pueden agrupar las actividades de auditoría a que deben someterse los dominios funcionales (ver apartado 4 de esta guía) sobre los cuales se desarrollará la auditoría.



En este sentido, para cada dominio funcional deberá asegurarse que los dominios de gestión han sido verificados, por ejemplo, para el caso del dominio de "formación y concienciación" se habrá de verificar si respecto de cada dominio funcional se han ejecutado los procesos de formación y concienciación orientados a que cada miembro de la organización esté suficientemente formado y/o concienciado en relación a sus funciones y responsabilidades.

Por supuesto cada organización deberá adaptar este esquema a su modelo de gestión del cumplimiento de la protección de datos.

A. Gestión de Riesgos

En las guías de análisis de riesgos[9] y de evaluaciones de impacto[10] publicadas por la Agencia Española de Protección de Datos (AEPD) se citaba textualmente el Considerando 74[11] del RGPD, indicando que cada actividad de tratamiento debe contar con unas medidas o controles que se habrán establecido en base al análisis de riesgo previo que se haya realizado sobre ese tratamiento según la naturaleza, ámbito, contexto y finalidades de dichos tratamientos.

En algunos tratamientos, que presenten un riesgo significativo (alto riesgo), habrá sido requerida una evaluación de impacto relativa a la protección de datos, pero en cualquier caso todos los tratamientos deberán ser objeto de una evaluación del riesgo, que deberá ser revisada y, en su caso actualizada, al igual que en el caso de las EIPD, de manera orientativa al menos con carácter anual, e incluso semestral, todo ello según el nivel de riesgo obtenido y la necesidad de mantenerlo controlado.

[9] "Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD" de la AEPD.
[10] "Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" de la AEPD.
[11] (74) *Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.*

Recomendamos trabajar tanto con indicadores cuantitativos como cualitativos, puesto que la gestión de riesgos, al plantear el cambio a un enfoque más preventivo que reactivo, requiere de ambos tipos de indicadores, en particular para evitar una aproximación excesivamente subjetiva.

Debemos entender cómo se realiza la función de ERM[12] en la compañía, si hay política de riesgos, si existe la función de CRO (Chief Risk Officer) y de CISO (Chief Information Security Officer), si real y efectivamente la toma de decisiones de los proyectos del último año ha incorporado esa gestión de riesgos, si hay un órgano que se preocupa por revisar esos riesgos y con qué regularidad, si existe un apetito de riesgo definido, si hay una planificación para mitigar esos riesgos, etc.

En este sentido, podemos utilizar indicadores según el riesgo que queramos verificar, por ejemplo, para verificar si las operaciones de tratamiento han sido objeto de evaluación de los riesgos, podemos verificar qué porcentaje de tratamientos del total tienen su informe de riesgos actualizado, o en relación a las evaluaciones de impacto, qué porcentaje han sido revisadas en el último ejercicio; los valores de cada indicador que pueden mostrar desviaciones, sobre lo que sería una situación aceptable deberán ser establecidos por la organización, en atención a las características de sus tratamientos.

B. Sistema de Gobernanza de la Privacidad

Por buen gobierno entendemos que haya unas políticas y procedimientos suficientes, que estén aprobados y actualizados y que toda la compañía los conozca, que haya unos roles y responsabilidades definidas tanto del DPD como de su modelo de relación con otras funciones clave, que haya un sistema de *reporting* definido y regular con la Alta Dirección, y que los objetivos estratégicos de la compañía estén alineados con la privacidad y la protección de datos.

El sistema de gobernanza de la privacidad es una de las piedras angulares para garantizar la continuidad del cumplimiento a lo largo del tiempo, que cristaliza en un proceso de cambio cultural progresivo de un enfoque reactivo a otro preventivo.

Dentro de esa gobernanza, además de la visibilidad, legitimidad y capacidades técnicas y financieras de que se dote al DPD, está su relación con otras funciones clave en el ámbito de control dentro de la empresa como: Calidad, Cumplimiento, Legal, Auditoría Interna, Tecnología de la Información, las Oficinas de Gestión de Proyectos (PMOs), Riesgos y Seguridad. Es fundamental haber documentado y aprobado unos modelos de

[12] Enterprise Risk Management.

interfaz (canales y protocolos) y de relación del DPD con cada uno de ellos, y entre sí.

Todos los dominios funcionales deben estar incluidos en esa gobernanza, por ejemplo, se podría verificar si el delegado de protección de datos dispone de presupuesto suficiente, o de los recursos humanos adecuados, o qué porcentaje del presupuesto de seguridad se destina específicamente a los tratamientos de datos de carácter personal.

C. Gestión Operativa

Por lo que respecta a la gestión operativa podemos usar indicadores que nos muestran el volumen de actividad que está suponiendo el proceso de gestión de la protección de datos dentro de una compañía, es decir, el peso que tienen los procesos vinculados a cada dominio funcional.

Un indicador esencial de la auditoría de este dominio de gestión sería comprobar si se cuenta con un cuadro de mando de indicadores que facilite la detección de riesgos puramente operativos como, por ejemplo, la respuesta al ejercicio de derechos, de manera que puedan establecerse umbrales de tiempo de respuesta o de satisfacción de los interesados respecto de sus solicitudes.

D. Gestión Documental

Una parte fundamental del cumplimiento está en poder demostrarlo y para ello debemos tener bien documentada la gestión operativa (normativas de contratos adaptados a nueva regulación y contratos actualizados, brechas de privacidad documentadas, bases legítimas como el consentimiento demostrables y auditables, políticas de privacidad aprobadas, procedimientos como derechos de información, identificación de tratamientos, notificación de brechas de privacidad, monitorización, gestión y análisis de riesgos, registros de formación, etc.

En este caso serán útiles indicadores que nos proporcionen información sobre la documentación actualizada en el último año, el control de versiones, la revisión de procedimientos, etc.

E. Formación y concienciación

La formación continua, la evaluación de esa formación y la concienciación regular mediante simulacros es una clara prueba del ejercicio de la responsabilidad proactiva y de

diligencia en el cumplimiento por parte de las compañías.

Aquí las organizaciones pueden disponer de indicadores tales como, del porcentaje de empleados que han superado la formación, el número de simulacros y empleados implicados, las consultas que han planteado durante el desarrollo de sus funciones y responsabilidades durante el último año, etc.

6.4. Valoración de la eficacia de los controles

En el presente apartado se describe el proceso de valoración de la madurez y eficacia de los controles implantados para gestionar las amenazas de incumplimiento y para la seguridad de los datos; esta valoración resulta particularmente necesaria en caso de que existan dudas sobre la eficacia de tales controles. El método de cálculo que se propone es meramente orientativo, y deberá ser adaptado a las necesidades y modelo de controles de cada organización.

Así, para valorar la madurez y la eficacia de los controles podemos usar ocho variables a las cuales se les ha asignado un valor, junto con un multiplicador para la verificación de la eficacia de los controles. Asimismo, los valores asignados a cada variable son sumatorios y el valor máximo que pueden alcanzar es quince.

Para estimar el valor de madurez del control se propone utilizar las siguientes variables:

1. El control es auditable, es decir, la medida de control puede ser verificada disponiendo de evidencias de cómo está implementado el control. [Variable AUDI].

2. El control está documentado, disponiendo de toda la documentación relativa al proceso de diseño, aprobación, implementación, etc. de la medida de control. [Variable DOCM].

3. El control está certificado, es decir, forma parte de un proceso de certificación llevado a cabo por terceros (como, por ejemplo, los certificados ISO). [Variable CERT].

4. Según si la ejecución del control o la medida de control depende de una persona concreta o de un grupo de trabajo. [Variable EJEC].

5. Según si se ha definido de manera clara al responsable de la medida de control. [Variable RESP].

6. Según si se realiza una monitorización continuada del control. [Variable MON].

7. Según si la medida de control está auditada de manera externa o interna. [Variable TIPAUD].

8. Según la vinculación del control, es decir, si la medida de control es consecuencia de un contrato u otro tipo de acuerdo. La eficacia del control se supone mayor, puesto que podrá someterse a verificación por parte de la contraparte. [Variable VINC].

AUDITABLE	DOCUMENTADO	CERTIFICADO	EJECUCIÓN
DEFINIR AL RESPONSABLE	MONITORIZACIÓN CONTINUADA	AUDITADA	VINCULACIÓN DEL CONTROL

Como se verá a continuación, se proponen unos valores a cada variable que, en función de la importancia de cada una de estas, será de 1 a 3 en caso de respuesta afirmativa y, en caso de respuesta negativa, siempre se le asignará el valor 0.

En la siguiente tabla se resumen los valores que, en función de las circunstancias, debe darse a cada una de las variables descritas, por supuesto son orientativos y el "peso" de cada variable se puede adaptar a las circunstancias y cultura de la organización:

VARIABLES PARA ANALIZAR LA MADUREZ DEL CONTROL	ID	DESCRIPCIÓN	SI/NO	VALOR
Auditable	AUDI	¿La medida o control se puede verificar?	SI	1
			NO	0
Documentada	DOCM	¿La medida o control adoptado está documentado?	SI	2
			NO	0
Certificada	CERT	¿La medida o control forma parte de un proceso certificado (por terceros)?	SI	3
			NO	0

VARIABLES PARA ANALIZAR LA MADUREZ DEL CONTROL	ID	DESCRIPCIÓN	SI/NO	VALOR
Ejecución	EJEC	¿La medida o control depende de una persona concreta o de un grupo de trabajo?	SI	1
			NO	0
Responsabilidad	RESP	¿Se ha definido claramente el responsable de la medida o control?	SI	2
			NO	0
Monitorización continuada	MON	¿Se realiza una monitorización continuada de la medida o control?	SI	2
			NO	0
Auditoría Externa/Interna	TIPAUD	¿La medida o control se auditada periódicamente de manera interna o externa?	SI	2
			NO	0
Vinculación	VINC	¿La medida o control es consecuencia de un contrato u otro tipo de acuerdo?	SI	2
			NO	0
			TOTAL	**15**

Junto con esas variables, hay que tener en cuenta también el denominado **multiplicador para la valoración de la eficacia del control** ("VEC"), que implica llevar a cabo una valoración cualitativa, teniendo en cuenta diferentes factores de implementación del control. Así, se aplicará la siguiente tabla para establecer su valor:

DESCRIPCIÓN	FORMA DE VERIFICACIÓN	VALOR (VEC)
El control está solo diseñado	Se disponen de informaciones sobre el diseño del control conforme está diseñado, pero no se encuentra implementado.	0
El control está diseñado e implementado	Se disponen de evidencias sobre la existencia e implementación del control, incluido su diseño.	1
El control está diseñado, implementado y correctamente configurado	Se ha verificado que el control está correctamente implantado (configurado), por lo que debería de cumplir eficazmente su función.	2

DESCRIPCIÓN	FORMA DE VERIFICACIÓN	VALOR (VEC)
El control está diseñado, implementado, con corrección configurado y funciona correctamente	Se ha verificado que cumple su función correctamente, en base a la disponibilidad de evidencias que lo confirman (pruebas o test).	3

Por tanto, para calcular la madurez y eficacia de los controles (MEC) se aplicará la siguiente fórmula:

MEC = (AUDI + DOCM + CERT + EJEC + RESP + MON + TIPDAUD + VINC) * VEC

El resultado de sumar las ocho variables de madurez de los controles y aplicarle el multiplicador a esa suma, estará entre 0 y 45, lo cual permitirá obtener una cuantificación numérica significativamente precisa del nivel de madurez y eficacia de los controles en materia de protección de datos personales con los que cuenta la compañía auditada.

Finalmente, para categorizar de una forma más intuitiva y ejecutiva la estimación de la madurez y eficacia de cada medida de control analizada, aplicaremos la siguiente escala, que también puede adaptarse a las circunstancias de cada organización, incluso incluyendo más niveles:

DESCRIPCIÓN DEL NIVEL DE EFICACIA DE LOS CONTROLES	VALORES DE CONVERSIÓN	NIVEL DE EFICACIA
NULA	0	0
REDUCIDA	≥ 1 - 17	1
ACEPTABLE	≥ 18 - 29	2
ALTA	≥ 30 - 45	3

6.5. Cálculo del nivel de cumplimiento

Para calcular el nivel de cumplimiento partiremos de las diferentes exigencias que se encuentran establecidas en las normas que regulan la protección de datos, y que, en nuestro caso, principalmente, son RGPD y LOPDGDD, pero sin olvidar otras normas sectoriales como serían LSSI[13] o LGTEL[14] , que también podrían ser de aplicación a la organización que es objeto de auditoría, y, en cuyo caso, el grado de cumplimiento de sus exigencias también debería ser objeto de evaluación.

[13] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
[14] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Por descontado si concurren otras normas sectoriales, que regulan aspectos relacionados con la protección de datos personales deberán ser tenidas en consideración.

Así, las exigencias establecidas en estas normas (RGPD y LOPDGDD) asociadas a los dominios funcionales podemos clasificarlas de la siguiente manera:

EXIGENCIAS NORMATIVAS	ARTÍCULOS
Gobierno de la Privacidad y Delegado de Protección de Datos	Arts. 37-39 RGPD; Arts. 34-37 LOPDGDD
Licitud y transparencia	Arts. 5-14 RGPD; Arts. 4-11, 19-25; Art.27 y 32 LOPDGDD
Gestión de Derechos	Arts. 15-22 RGPD, Arts. 12–18, Art. 89 y Art. 90 LOPDGDD
Privacidad por diseño y defecto	Art. 25 RGPD
Registro de actividades de tratamiento	Art.30 RGPD; Art.31 LOPDGDD
Análisis de riesgos y evaluaciones de impacto de la protección de datos	Arts. 35 y 36 RGPD; Art. 28 LOPDGDD
Notificación de Brechas de seguridad de datos personales	Art.33-34 RGPD
Medidas de seguridad	Art.32 RGPD;
Responsabilidad proactiva *Accountability*	Arts. 5.2, 24 RGPD; Arts. 28-32 LOPDGDD
Encargados de tratamiento	Art. 28 RGPD; Art. 33 LOPDGDD;
Transferencias internacionales	Arts. 44-49 RGPD: Arts. 40-43 LOPDGDD
Corresponsabilidad	Art. 26 RGPD; Art.29 LOPDGDD

Una vez que hemos identificado las exigencias normativas, analizaremos las evidencias y documentación existente relacionada con dichas exigencias y con las medidas que se hayan planificado e implantado para llegar a su cumplimiento, lo que nos permitirá evaluar el nivel de cumplimiento de cada una ellas.

La evaluación del nivel de cumplimiento estará vinculada por un lado al grado de eficacia de las medidas, y al hecho de si el conjunto de medidas previstas para cada dominio

funcional da respuesta a todos los requisitos de cumplimiento que se derivan de los principios, derechos y obligaciones previstos en la regulación.

Deberemos preguntarnos:

¿Tenemos suficientes controles para cumplir con cada dominio funcional?
Visión de conjunto.

¿Cada control implantado es eficaz en sí mismo?
Visión individualizada.

Así como ya hemos planteado que, para el cálculo de la eficacia de los controles, podemos recurrir a una serie de variables que nos permiten objetivar hasta qué punto un control específico puede dar un resultado adecuado al objetivo de control que persigue, para determinar si disponemos de los controles necesarios para cumplir con cada dominio funcional, habrá que usar una valoración más cualitativa, sustentada en el criterio experto.

Lo óptimo sería poder combinar el valor de la eficacia de los controles (individualmente) y de la suficiencia del conjunto de todos ellos por dominio funcional (conjuntamente) para, en base a una escala de nivel de cumplimiento, poder situar en qué situación se encuentra la organización respecto del cumplimiento; por ejemplo, aplicando una tabla como la que se refleja a continuación:

NIVELES DE CUMPLIMIENTO	
Cumplimiento muy bajo	0%-10%
Cumplimiento bajo	11%-50%
Cumplimiento medio	51%-80%
Cumplimiento alto	81%-90%
Cumplimiento muy alto	91%-100%

Para obtener el nivel global de cumplimiento de la organización, realizaremos una ponderación de los niveles de cumplimiento de cada una de las exigencias normativas identificadas, obteniéndose de esta forma el nivel del cumplimiento global.

Una vez que hayamos calculado el nivel de cumplimiento, podremos detectar las deficiencias de cumplimiento en dominios funcionales concretos y diseñar e implementar aquellas medidas que, con su eficacia, permitan corregir dichas situaciones a fin de reducir el riesgo de incumplimiento que se haya detectado.

Para ello, actuaremos sobre las áreas de la organización donde radiquen aquellas deficiencias de cumplimiento que hayamos identificado, para que se tomen las decisiones oportunas para mejorar el nivel de cumplimiento.

6.6. Análisis de los resultados

En base al nivel de cumplimiento expuesto en el apartado anterior, pondremos el foco sobre todo en los dominios auditados donde hayamos obtenido un % de cumplimiento inferior al 50% puesto que todo aquello que esté por debajo de ese nivel debe suponer una recomendación con prioridad alta en cuanto a la necesidad de actuar para mejorar ese nivel de cumplimiento.

Aquello que se sitúe entre un 50 y un 80% de cumplimiento y que suponga un cumplimiento medio debe tratarse como una recomendación con prioridad media, dejando ya como sugerencias de mejora y posibles "best practices" los controles que por su implementación y eficacia cumplan más del 80% de los muestreos o del dominio auditado.

A la hora de analizar los resultados debemos categorizar y ordenar en base a la prioridad en la aplicación de las acciones de mejora en el informe de recomendaciones. Para graduar la prioridad de la recomendación debemos tener en cuenta si en esos resultados de las pruebas de auditoría y controles, se da algunas de las siguientes diez variables:

VARIABLE	CUESTIÓN	SI/NO
Antigüedad desde identificación	¿Esa debilidad de control ya fue detectada en pasadas auditorías de protección de datos (aquí recomendamos siempre solicitar el último informe de auditoría) o en el plan de Adecuación a RGPD y todavía no se ha subsanado?	
Tratamiento a gran escala	¿El tratamiento donde tiene lugar esa debilidad de control estaría tipificado como *Tratamiento a gran escala* (véase definición de *Tratamiento a gran escala en dictamen WP 248* del GT29 sobre la Evaluación del Impacto de la Protección de Datos (EIPD), que remite a su vez al dictamen WP 243, o el considerando 91 RGPD)?	
Graduación de la sanción	¿Qué tipo de infracción puede suponer este no cumplimiento (véase art. 83.2 del RGPD) siendo determinantes número afectados, tipo de datos afectados, duración del incumplimiento, intencionalidad, lucro obtenido por ello, infracciones o sanciones efectivas anteriores por ese mismo motivo, quejas formales recibidas vía Defensa del Cliente/OCUs, etc.?	
Colectivos en situación de vulnerabilidad	¿El incumplimiento de esos controles está afectando a datos de menores (14 años según LOPDGDD) o colectivos en riesgo de exclusión social (discapacidad, edad avanzada, niños bajo tutela, inmigrantes, desempleados, víctimas de violencia de género, etc.)?	
Tipificado como prohibido	¿Está prohibido directamente por el RGPD o la LOPDGDD (ej: bases de datos de antecedentes penales, elaboración de perfiles que dé lugar a una discriminación de las personas físicas basándose en las categorías especiales de datos personales, etc.)?	
Finalidad del tratamiento	¿Los datos se han utilizado para una finalidad manifiestamente distinta a la informada al interesado?	
Inexistencia de función de DPD o similares	¿La Alta Dirección de esa compañía no ha nombrado un Delegado de Protección de Datos (interno o externo) o no tiene ninguna función relacionada con ámbito de control, calidad, seguridad, auditoría que ayude a que las acciones de mejora detectadas se ejecuten y se dé un seguimiento?	
Falta de Transparencia	¿Se observa que hay una intencionada falta de transparencia, obstaculización u omisión reiterada al ejercicio de los derechos del interesado? O peor aún, si se ha observado por el auditor obstaculización a la realización de las pruebas necesarias en el transcurso de la auditoría para poder obtener más información sobre el hallazgo.	
Desatención de asesoramiento previo DPD o de la Autoridad de Control	¿Se demuestra que la Alta Dirección ha desoído a los consejos de asesoramiento al respecto de ese incumplimiento por parte del Delegado de Protección de Datos y o peor aún, hay incumplimiento frente a resoluciones ya dictadas previamente por la AEPD a esa compañía?	
Brechas de protección de datos ligadas al incumplimiento	¿Existen ya brechas de privacidad declaradas e incidencias de seguridad registradas fruto de dicho incumplimiento?	

Si el incumplimiento por el deficiente diseño del control, o su inefectiva implementación en la compañía es muy bajo o bajo y se añade que confluyan algunas de las variables enumeradas, implicará una recomendación con prioridad muy alta e incluso crítica (hasta el punto de no poder continuar la auditoría hasta que se plantee una acción de mejora y se empiece a realizar).

También debemos considerar estas otras variables de cara a priorizar más niveles de cumplimiento que quedan en estado medio e incluso alto, porque la no realización de esas acciones de mejora puede implicar que se deteriore el resultado de la auditoría y que en las sucesivas que se realicen, donde antes había un cumplimiento medio luego pueda tipificarse como bajo por el factor de antigüedad/duración del incumplimiento.

NIVEL DE CUMPLIMIENTO	CATEGORÍA	PRIORIDAD ACCIÓN DE MEJORA	PLAZOS REMEDIACIÓN (ORIENTATIVO)
Muy bajo (0- 10%)	Inefectivo	Crítico	Acción Inmediata/ no puede concluir la Auditoría hasta su cierre
Cumplimiento bajo (11%-50%)	Poco Efectivo	Muy Alta	3 meses
Medio (51-80%)	Efectivo con Retricciones	Alto	6 meses
Alto (81-90%)	Satisfactorio	Medio	1 año
Muy alto (91-100%)	Efectivo	Bajo	No requiere acción

Remarcar que hay múltiples modelos de priorización de los resultados y sus acciones de mejora, si bien aconsejamos tender a utilizar modelos que no nos lleven a zonas de confort intermedias, para valorar los resultados obtenidos tras el análisis cuantitativo de las pruebas de auditoría, utilizando escalas pares que hacen que nos cueste decantarnos por la opción neutral (por ejemplo: si utilizamos una escala del 1 al 7 tenderemos a ir al 4, mientras que si usamos del 1 al 6 nos permitirá reflexionar más sobre si nos situamos en un 3 o un 4).

Si se encuentran hallazgos durante las pruebas de auditoría, el auditor debe aumentar la muestra, para tener más evidencias que le permitan confirmar y asegurar que el incumplimiento de ese control es manifiesto y repetitivo.

También en este sentido es importante antes de priorizar, adelantar al interlocutor dicho hallazgo, para que nos ayude a contextualizarlo y saber si efectivamente dentro de la organización tiene un impacto o no, detectar posibles controles compensatorios que minimicen dicho incumplimiento o lo maticen de cara al informe de recomendaciones, etc. La empatía en este sentido por parte del auditor es fundamental en este punto, sin que obviamente esto pueda hacer cambiar el criterio del auditor al respecto.

Con todo esto pasaremos a diseñar el informe de Auditoría con su plan de acciones de mejora consensuadas o incorporando al menos los comentarios de la compañía auditada.

07

Emisión del Informe

7.1. Objetivo y ventajas del Informe de Auditoría

Con carácter general, el Informe de Auditoría, (en adelante, IA), se configura como un medio o instrumento para informar, con carácter general, a la Alta Dirección de la Organización sobre el grado de cumplimiento de los procesos y procedimientos que tiene implantados, en relación a los requerimientos normativos aplicables en cada momento. En definitiva, el IA sería el resultado del proceso específico de evaluación del grado de cumplimiento normativo de medidas de todo tipo, implementadas por una organización, para el cumplimiento de las normas que le son de aplicación.

Desde una perspectiva focalizada en la protección de los datos personales, el IA es una herramienta válida y eficaz que permite al Delegado de Protección de Datos u órgano de gobierno en materia de protección de datos, por un lado, realizar una correcta valoración del riesgo de los procesos y procedimientos y su alineamiento con la normativa aplicable y, por otro, informar del nivel de cumplimiento normativo a la Alta Dirección de la entidad.

7.2. Contenido del Informe de Auditoría y claves en su elaboración

La Norma ISO 19011 – 2018 relativa a las *Directrices para la Auditoría de los Sistemas de Gestión*, (en adelante, ISO 19011), en su apartado 4, establece en los "Principios de Auditoría", punto b), que: *los hallazgos, conclusiones e informes de la auditoría deberían reflejar con veracidad y exactitud las actividades de auditoría. Se debería informar de los obstáculos significativos encontrados durante la auditoría y de las opiniones divergentes sin resolver entre el equipo auditor y el auditado. La comunicación debería ser veraz, exacta, objetiva, oportuna, clara y completa*.

Por su parte, la *Guía de Seguridad de las TIC CCN-STIC 802*, elaborada por el Centro Criptológico Nacional, define el Informe de Auditoría como: *el producto final de las tareas realizadas en una auditoría. En el informe el auditor comunica, a quien corresponda, los resultados de las tareas realizadas, con los resultados obtenidos*.

En todo caso, el IA deberá ser un fiel reflejo del proceso de auditoría que se ha realizado y deberá documentarse describiendo fielmente las labores y acciones realizadas, las evidencias que respaldan dichos hallazgos y los resultados y conclusiones de dicho proceso.

7.2.1. Información que permita contextualizar la Auditoría realizada

Equipo auditor y metodología empleada

El equipo auditor es una de las piezas claves en todo proceso de revisión, por lo que deberá estar formado por personal para cuya elección se hayan tenido en cuenta criterios que permitan, no sólo garantizar el conocimiento experto y actualizado de la materia a auditar (en el caso que nos ocupa toda la normativa en materia de protección de datos), sino también contar con experiencia demostrable para una correcta manipulación de las evidencias de auditoría.

Adicionalmente, es imprescindible que se trate de un equipo multidisciplinar dotado, por un lado, de profesionales con conocimientos jurídicos especializados en protección de datos y, por otro, de profesionales técnicos con conocimientos especializados en seguridad informática. Por ello, configurar un buen equipo de auditoría requiere considerar factores de evaluación precisos y demostrables, razón por la que puede ser recomendable que sus miembros cuenten con alguna certificación nacional o internacional que permita verificar, a priori, su preparación (p.e. Certified Data Privacy Professional, CDPP, Certified Information Privacy Professional, CIPP, Certificación CISA, ISO 27001 Lead Auditor, Certificación del Esquema Nacional de Seguridad, etc.). Igualmente, se deberá comprobar la correspondiente experiencia en la materia.

Con relación a su tamaño, el número mínimo de personas que lo formen debe estar directamente relacionado con el tamaño de la organización/área/centro a auditar. En todo caso, cada miembro deberá desempeñar un rol específico dentro de dicho equipo (supervisión, realización, emisión y resultados), que será asignado por el líder del equipo auditor y según lo especificado por la ISO 19011 en su apartado 6.3.3 "Asignación de las tareas del equipo auditor", según el cual: *tales asignaciones deberían tener en cuenta la imparcialidad, la objetividad y la competencia de los auditores y el uso eficaz de los recursos, así como los diferentes roles y responsabilidades de los auditores, los auditores en formación y los expertos técnicos*.

EQUIPO DE AUDITORÍA	Debe proteger la **integridad** y **trazabilidad de la información** que se ha utilizado como base del informe de auditoría.

Uno de los puntos fundamentales que nunca podrán ser quebrantados es que sus miembros no hayan participado anteriormente de manera directa en la adecuación e implantación de las medidas y requisitos en los sistemas de información y/o tratamientos, de forma que goce de una total y real independencia que le permita garantizar la emisión de juicios libres e imparciales y que adolezcan de cualquier juicio de valor que no sea objetivo.

Además del requisito anterior, hay que poner de relieve que el Delegado de Protección de Datos de la organización/área/centro a auditar tampoco podrá realizar o participar activamente en el proceso de revisión, ya que ello podría poner en peligro su independencia (máxime cuando parte de la auditoría será revisar las funciones del DPD y así lo especifica el propio art. 39.1b) del RGPD al establecer entre sus funciones la de: *supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes*.

DELEGADO DE PROTECCIÓN DE DATOS

Su papel se circunscribe únicamente a **supervisar la realización de la Auditoría** debiendo garantizar que las conclusiones lleguen al órgano encargado de proponer y/o implantar acciones que puedan derivarse de las posibles no conformidades detectadas.

No obstante lo anterior, la ISO 19011 contempla la figura del "observador" entendido como aquella "persona que acompaña al equipo auditor (3.14) pero no actúa como un auditor". Según dicha Guía: *los guías y los observadores pueden acompañar al equipo auditor con la aprobación del líder del equipo auditor, del cliente de la auditoría y/o del auditado, según se requiera. Ellos no deberían influir ni interferir en la realización de la auditoría. Si esto no se puede asegurar, el líder del equipo auditor debería tener el derecho de negarse a que los observadores tomen parte en ciertas actividades de auditoría* (punto 6.4.2). Además, tal como establece la *Guía de Seguridad de las TIC CCN-STIC 802* elaborada por el Centro Criptológico Nacional: *el observador puede designarse por el auditado, una autoridad reglamentaria u otra parte interesada que testifica la auditoría*, por lo que esta figura, sí podría ser asumida por el DPD durante el desarrollo de la auditoría ya que

su observancia no influye ni interfiere en la realización de la misma.

En lo que respecta a la metodología de auditoría empleada durante la realización de la misma, se deberán especificar los métodos utilizados, tal y como recoge la ISO 19011 en su apartado 5.5.3 "Selección y determinación de los métodos de auditoría", estableciendo que: *Las personas responsables de la gestión del programa de auditoría deberían seleccionar y determinar los métodos para llevar a cabo la auditoría de manera eficaz y eficiente, dependiendo de los objetivos, el alcance y los criterios de la auditoría definidos*.

Es imprescindible especificar si se ha realizado in situ, de forma remota o ha sido una combinación de ambas.

Personal entrevistado y áreas auditadas

Es de vital importancia identificar la persona a la que se ha auditado y el área a la que pertenece, incluyendo sus datos de contacto por si la Dirección o responsables de la organización/área/centro auditado tuvieran que dirigirse a éste. Así mismo, también se habrá de identificar a aquellas personas o áreas a las que no se ha podido auditar por algún motivo justificado.

Objetivos y ventajas del IA

El IA tiene como principal misión la de dictaminar de forma objetiva el grado de cumplimiento (total o parcial) de la normativa en materia de protección de datos personales, de las medidas legales, organizativas y controles técnicos de seguridad implantados en la organización/área/centro auditado.

Por ello, el IA tiene como principales objetivos los siguientes:

- Por un lado, **detallar los aspectos relevantes detectados** en la organización/área/centro auditado con orientación al riesgo de incumplimiento en materia de protección de datos personales.

  Esto es, especificar los incumplimientos y debilidades detectadas en la organización/área/centro auditado, lo cual permitirá a la Dirección o a los responsables conocer el grado de adecuación real a las obligaciones normativas y conocer los riesgos a los que se enfrenta dicha organización/área/centro auditado, en caso de que sus incumplimientos y debilidades no sean subsanados. Por ello, se deberán acompañar de datos, hechos y observaciones en los que se basen las conclusiones alcanzadas.

En el mismo sentido, además de identificar incumplimientos y debilidades confirmados, se deberán incluir las recomendaciones por parte del equipo auditor.

- Por otro lado, **trasladar** a la Dirección o responsables de la organización/área/centro auditado **la relevancia de las conclusiones y el beneficio de corregir las debilidades** detectadas o el perjuicio, en caso contrario.

Para conseguir una estructura clara y que ayude a la fácil comprensión de los destinatarios del mismo, que no es otro que la Dirección o responsables de la organización/área/centro auditado, puede ser recomendable agrupar los incumplimientos o debilidades detectadas en función de las tipologías de materias auditadas, estableciendo apartados diferenciados para los incumplimientos materias cuyo componente sea legal, organizativo y técnico.

En lo que respecta a los beneficios que reporta la elaboración del IA, entre otros, se podrían destacar los siguientes:

BENEFICIOS DEL IA

- **Elevar el grado de cumplimiento** a través de la implantación de medidas que minoran el riesgo de incumplimiento.
- **Demostrar el compromiso** por el cumplimiento normativo de la organización/área/centro auditado al establecer controles de cumplimiento periódicos.
- **Conocer, de forma veraz y actualizada el estado de cumplimiento** de la organización/área/centro auditado en materia de protección de datos.
- **Permitir la verificación real de la implantación y cumplimiento** de los requisitos exigidos por la normativa aplicable en materia de Privacidad, además de cumplir con uno de los pilares fundamentales sobre los que se sustenta cualquier sistema basado en el ciclo de mejora continua (Plan *Do-Check-Act*) que en definitiva es lo que parece que intenta promulgar la actual normativa en materia de Privacidad.
- **Ayudar a reforzar la imagen y reputación corporativa** de la organización/área/centro auditado.
- **Poner a prueba la organización/área/centro auditado** porque no se realiza ningún tipo de control, podrían producirse incumplimientos que difícilmente podrían ser detectados.
- **Permite descubrir oportunidades de mejora** de forma incirecta.

Alcance del IA

El alcance es uno de los puntos que deben quedar claramente delimitados de forma previa a la realización de cualquier auditoría. Si bien, aunque el alcance ha debido ser delimitado de forma previa, es de suma importancia que en el propio IA se detallen minuciosamente los siguientes puntos que nos permitan contextualizar el alcance real de la auditoría realizada:

- Delimitación del ámbito afectado, especificando si se trata de una organización/área/centro o, por el contrario, si es a un grupo de empresas o conjunto de áreas o centros.
- Lugar de ubicación de la organización/área/centro auditado.
- Requisitos regulatorios sobre los que se ha realizado la revisión. No sólo habrá que hacer referencia a la normativa europea y local que resulte de aplicación en materia de protección de datos, sino también habrá que detallar las políticas y normativas internas que la organización/área/centro tenga desarrolladas e implantadas en materia de protección de datos (o materias relacionadas).
- Fechas durante las que tuvo lugar la auditoría.
- Tratamientos de datos personales y sistemas informáticos auditados.
- Estructura de gobierno en materia de protección de datos existente en la organización/área/centro auditado. Puede ser recomendable (aunque no obligatorio) especificar las personas que forman parte de dicha estructura por cuanto que puede ayudar a contextualizar el modelo de gestión adoptado por la organización para el cumplimiento en materia de protección de datos.
- Las medidas de seguridad a auditar, entre ellas, la auditoría puede abarcar medidas de naturaleza diversa (organizativa, física y lógica, entre otras).

Por lo tanto, como parte de la definición del alcance de la auditoría, es necesario con carácter previo a su comienzo, identificar los elementos que entran dentro de ésta.

Además, tal y como recomienda la ISO 19011 en su apartado 6.5.1 "Elaboración del Informe de Auditoría", el IA también puede incluir (como hemos recomendado anteriormente): *cualquier área dentro del alcance de la auditoría no cubierta, incluyendo cualquier cuestión sobre la disponibilidad de las evidencias, los recursos o la confidencialidad, con las justificaciones relacionadas*.

Por su parte, la *Guía de Seguridad de las TIC CCN-STIC 802* elaborada por el Centro Criptológico Nacional define las "limitaciones al alcance" como: *aquellos registros o documentos, o elementos del alcance de la auditoría, a los que, aunque previstos en las revisiones planificadas, para lograr los objetivos de la auditoría, el auditor no ha podido tener acceso por distintas razones, y cuya restricción de acceso puede impactar en las conclusiones de la auditoría. Estas deben estar reflejadas en el informe de auditoría,*

En el contexto de esta guía de auditoría, esta situación debería ser excepcional, aunque puede darse el caso de que las restricciones surjan en la fase inicial de delimitación del alcance. El auditor deberá indicarlo en el informe final y en la planificación. Asimismo, si surge en la fase inicial, debe indicarse el posible impacto en la realización de la auditoría, y la obtención de las conclusiones en relación al objetivo de la auditoría. Es conveniente que, en todos los casos, el auditor requiera que se comunique por escrito la restricción de acceso a registros, documentos o elementos auditables, y justificados por el objetivo de la auditoría.

También es importante detallar cuáles son aquellos sistemas, operativas y procedimientos que no han podido ser revisados a pesar de poderse encontrar en el alcance inicial de la misma y la argumentación de aquellos motivos por los que no haya sido posible dicha revisión.

Procedimientos de auditoría utilizados y criterios de selección de muestras

Tal y como establece la *Guía de Seguridad de las TIC CCN-STIC 802* elaborada por el Centro Criptológico Nacional, los procedimientos de auditoría: *comprenden el proceso de auditoría: habitualmente aluden a los procesos relacionados con la definición de las pruebas, su planificación y su ejecución*.

Los procedimientos o técnicas de auditoría a utilizar, entre otros, podrán ser los siguientes:

1. Realizar entrevistas directamente al personal auditado.
2. Completar cuestionarios con ayuda del auditado.
3. Observar y verificar el cumplimento de la operativa y de los procedimientos realmente implantados.
4. Utilizar técnicas de rastreo o trazabilidad.
5. Analizar el contenido de la normativa y procedimientos internos.
6. Revisión documental.
7. Realizar inspecciones oculares que requieren un examen físico de activos

tangibles o de hechos.

8. Realización de pruebas técnicas.

9. Obtención y revisión de evidencias de controles, etc.

A eso se podrá añadir la realización de pruebas selectivas o pruebas por muestreo. En este último caso, es necesario tomar como base un conjunto de muestras que sean representativas, de forma que permita llegar a conclusiones lo más parecidas posible a las que alcanzaríamos si hubiéramos evaluado todos los casos.

La determinación de los procedimientos de auditoría concretos a utilizar dependerá de la decisión del auditor, en base a varios factores. Lo importante será plasmar de forma clara los procedimientos elegidos, así como el tipo de evidencia que ha surgido de la técnica utilizada.

En definitiva, la documentación y evidencias analizadas debe ser la suficiente que hubiera permitido a un tercero independiente obtener los mismos resultados.

Puntos divergentes sin resolver

En todo IA es necesario dejar un apartado en el que especificar aquellos puntos sobre los que no se ha conseguido un consenso entre el equipo auditor y el auditado o el Delegado de Protección de Datos u órgano de gobierno en materia de protección de datos.

Fecha y firma

Es imprescindible detallar la fecha de emisión del IA, así como la identificación del auditor responsable, que firma (y, en consecuencia, ratifica) los resultados obtenidos durante el proceso de auditoría.

7.2.2. Conclusiones

El IA podrá incluir un apartado destinado a la exposición de los resultados de los trabajos llevados a cabo en el marco de la auditoría. Bajo epígrafes tipo "Conclusiones" o "Resultados", el auditor concretará el análisis realizado.

De acuerdo con lo establecido en la ISO 19011: *el contenido de las conclusiones de la auditoría debería tratar aspectos tales como los siguientes: a) El grado de conformidad con los criterios de auditoría y la robustez del sistema de gestión, incluyendo la eficacia del sistema de gestión para cumplir los resultados previstos, la identificación de riesgos*

y la eficacia de las acciones tomadas por el auditado para abordar los riesgos; b) La implementación, el mantenimiento y la mejora eficaces del sistema de gestión; c) El logro de los objetivos de la auditoría, cobertura del alcance de la auditoría y cumplimiento de los criterios de la auditoría; d) Hallazgos similares encontrados en distintas áreas auditadas o en una auditoría conjunta o en una auditoría previa, con el propósito de identificar tendencias. Si se especifica en el plan de auditoría, las conclusiones de auditoría pueden llevar a recomendaciones para la mejora, o a futuras actividades de auditoría.

En el entendido de que el IA se constituye como un elemento eficaz y necesario para informar a la Alta Dirección de la Organización sobre el grado de cumplimiento de la normativa sobre protección de datos de carácter personal aplicable, se considera muy recomendable que el IA sea preciso, claro y conciso. La utilización de formatos con gran contenido visual, facilita la lectura y comprensión, y permiten identificar rápidamente el resultado final del informe.

En ese sentido, el uso de colores junto con una leyenda explicativa, constituye una forma más que idónea para mostrar de manera ágil y clara el resultado de la AI.

Ejemplo:

Este apartado podrá completarse además mediante una exposición sencilla o un listado de las debilidades detectadas, junto con el grado de impacto en el objeto de la IA.

La utilización también de colores, símbolos o cifras facilitará la valoración final del informe en términos de impacto y riesgo derivado:

DEBILIDAD MODERADA

DEBILIDAD SIGNIFICATIVA

Además de la relación de las debilidades detectadas, se considera oportuno acompañar, al menos, la siguiente información, que permitirá completar la valoración del riesgo por parte del Delegado de Protección de Datos u órgano de gobierno en materia de protección de datos:

- Detalle del evento que supone una actuación conforme o alineada con lo dispuesto en la normativa de aplicación.

  En relación con este apartado, se tendrán en cuenta el estado de los procesos, la existencia de procedimientos, el grado de cumplimiento por parte de los responsables o partícipes en el mismo, así como la eficacia de sus resultados.

- Identificación del acto o hecho que implica un posible incumplimiento normativo.

  En estos casos resultará muy conveniente además la identificación de la disposición normativa afectada, así como una valoración sobre el impacto teniendo en cuenta el ánimo sancionador de la autoridad de control o el catálogo de infracciones de la LOPDGDD. Los incumplimientos o no conformidades con la norma, podrán clasificarse teniendo en cuenta el contexto específico de la Organización y su modelo de gestión del riesgo.

- Opinión del Auditor, que deberá ser objetiva e independiente.

  Comprenderá una visión global del cumplimiento de los requisitos regulatorios, indicando el grado de cumplimiento de los mismos. Podrá incluir, asimismo, una exposición resumida de las acciones llevadas a cabo por la organización en aras al cumplimiento de la norma. En particular, la opinión del auditor se focalizará en una exposición de los aspectos de mejora relacionados con las debilidades detectadas en el marco del trabajo llevado a cabo. En este apartado "Conclusiones" bastará con una breve explicación de estas medidas que serán objeto de desarrollo en el apartado 7.4. denominado "Plan de Acción" de esta Guía.

7.2.3. Evaluación de la mejora continua

Aunque el RGPD no ha entrado a regular el régimen de las auditorías de protección de datos, es habitual y conveniente que los trabajos de auditoría sean recurrentes, máxime en estos primeros años de cumplimiento del RGPD, que exigen una continua revisión del cumplimiento de las entidades, públicas o privadas, en materia de protección de datos.

Poniendo el énfasis en esa continua revisión, no deberíamos considerar las auditorías

de protección de datos como hechos aislados, que componen fotografías fijas de los estados del nivel de cumplimiento normativo en materia de protección a las fechas en que se realicen cada una de las auditorías, sino como parte de un proceso continuo de seguimiento eficaz que toda entidad, pública o privada, estaría obligada a llevar si quiere cumplir con el RGPD, y poder demostrarlo.

Tal y como establece la ISO 19011 en su apartado 6.7,: *los resultados de la auditoría pueden indicar la necesidad de correcciones o de acciones correctivas, u oportunidades para la mejora. Tales acciones generalmente son decididas y emprendidas por el auditado en un intervalo de tiempo acordado. Cuando sea apropiado, el auditado debería mantener informadas a las personas responsables de la gestión del programa de auditoría y/o al equipo auditor sobre el estado de estas acciones*.

> *Debería verificarse si se completaron las acciones y su eficacia. Esta verificación puede ser parte de una auditoría posterior. Debería presentarse un informe con los resultados a la persona responsable de la gestión del programa de auditoría, y al cliente de la auditoría para la revisión por la dirección.*

Por tanto, además de una herramienta de ayuda para el Delegado de Protección de Datos, u órgano de gobierno en materia de protección de datos, y de información del nivel de cumplimiento normativo en materia de protección de datos a la Alta Dirección, la auditoría de protección de datos deberían ser un instrumento de las entidades, públicas o privadas, ya sean responsables o encargadas, de seguimiento y verificación del estado de dichas acciones correctivas que se han planificado a raíz de la detección de errores o no cumplimientos en los resultados de las auditorías que la han precedido.

En consecuencia, el IA deberá tener en cuenta las auditorías realizadas anteriormente por dichas entidades, que no deben ceñirse solo a las internas, sino que podrían también abarcar las auditorías externas, para ir recogiendo formalmente en cada última auditoría practicada la evolución acontecida en la entidad auditada en materia de protección de datos, mediante la comparación de los resultados ofrecidos por las auditorías anteriores.

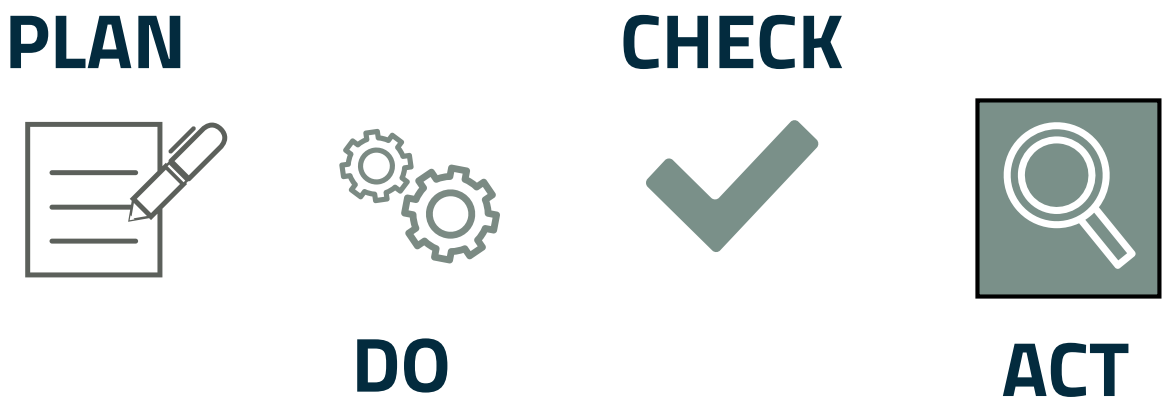
Además de los resultados de las auditorías precedentes, el IA deberá recoger:

1. Las acciones correctivas recomendadas en los planes de acción de las auditorías.
2. Si dichas acciones han sido asumidas por la entidad auditada.

3. Si se han realizado auditorías de RGPD previas, si se han completado o el estado de estas acciones a la fecha en que se ha realizado esta última auditoría.

4. La verificación de la eficacia de dichas acciones acometidas por la entidad auditada en su grado de cumplimiento normativo en materia de protección de datos.

De esta forma el IA permitirá a la entidad auditada documentar la aplicación de un sistema basado en el ciclo de mejora continua (Plan *Do-Check-Act*) en materia de protección de datos, que como ya hemos expuesto anteriormente resulta fundamental para demostrar el grado de compromiso de las entidades, públicas y privadas, en el cumplimiento de la nueva normativa, constituyéndose como mejores prácticas, que seguro serán tenidas en cuenta por la autoridad de control en los casos de aplicación del régimen sancionador.



No obstante, para ser realistas, en el IA el auditor deberá tener en cuenta que es poco probable que la organización pueda completar todas las acciones de mejora o correctoras al mismo tiempo, dado los recursos y tiempo que requiere cada acción. Por lo tanto, el IA, para una mejor valoración, deberá contemplar si la entidad auditada las ha organizado por orden de prioridad y si se están cumpliendo los objetivos de corrección o mejora dentro del contexto específico de la entidad auditada.

De esta forma, los IA podrán servir como método del seguimiento cronológico de la evolución en el cumplimiento normativo de las entidades auditadas, con especial seguimiento de los planes de acción asumidos para subsanar posibles deficiencias o incumplimientos y los resultados que han tenido dichos planes.

Cuando se trate de una auditoría de protección de datos efectuada por primera vez a una entidad, el papel del responsable de esta primera auditoría adquiere una especial relevancia al dejar sentados los programas y estructura de la estrategia a seguir en las siguientes auditorías.

7.3. Estadios del Informe de Auditoría: Informe Preliminar e Informe Definitivo

Una vez completado el proceso de auditoría de protección de datos, entramos en la última fase del IA, como es la redacción y emisión del Informe Definitivo, con la previa redacción de un IA Preliminar, momento en el que puede tener sentido la intervención del Delegado de Protección de Datos para ejercer algunas de las funciones que le atribuye el RGPD, en su art. 39.1b, como son las de supervisar el cumplimiento de lo dispuesto en las normativas de protección de datos y las políticas de las entidades, responsables o encargadas.

Como se exponía en el anterior apartado, hasta este momento, el Delegado de Protección de Datos solo ha podido ejercer la función de "supervisar las auditorías correspondientes", establecida en el citado artículo, sin interferir en la realización de la auditoría para no poner en peligro la independencia de la auditoría.

Que las funciones del Auditor y las del Delegado de Protección de Datos están diferenciadas, lo demuestra el hecho de que las conclusiones de un Auditor en un IA pueden verse contradichas por las opiniones o dictámenes del DPD u órgano de gobierno de la privacidad.

Con la redacción del primer borrador de IA, el auditor debe ofrecer al Delegado de Protección de Datos y a las partes auditadas de la organización la posibilidad u opción de corregir cualquiera de las inconsistencias que a su juicio hubieran podido detectar o proceder a las aclaraciones que pudieran suscitarse.

Tanto el auditor como el Delegado de Protección de Datos y las partes auditadas, harán el mayor esfuerzo posible para aclarar conjuntamente dichas inconsistencias o disconformidades, siendo deseable que el IA que llegue a la Alta Dirección cuente con el máximo consenso.

No obstante, pudiera darse el caso de que el Auditor no aceptara dichas opiniones o aclaraciones y no quisiese acceder a su corrección en el IA Definitivo, en cuyo caso, pudiera ser una posibilidad, dependiendo de la dimensión de la organización auditada y

del tipo de auditoría que se esté llevando a cabo, ofrecer un espacio en el mismo IA Definitivo para formular, a modo de "voto particular", las disconformidades o aclaraciones siendo el Delegado de Protección de Datos el encargado de recopilarlas formalmente en el IA, en aras de cumplir con el objetivo de realizar una correcta valoración del nivel de cumplimiento normativo en materia de protección de datos para informar a la Alta Dirección.

En consecuencia, las características propias de los dos estadios de un IA de Protección de datos, serán:

IA Preliminar

- Elaboración del IA preliminar: el auditor presentará un borrador de trabajo o informe preliminar, con base en las observaciones y conclusiones que se obtengan durante la fase de ejecución de la auditoría.

- Revisión y validación del IA preliminar: el área o partes auditadas y el Delegado de Protección de Datos u órganos de gobierno en materia de protección de datos, podrán revisar y solicitar al auditor las aclaraciones que consideren oportunas sobre el contenido del IA Preliminar y, en particular, en relación con las debilidades detectadas y a las medidas correctoras propuestas. Será en ese momento, cuando los intervinientes hagan un esfuerzo y lleguen a un acuerdo para hacer llegar a la Alta Dirección un IA sin disconformidades en cuanto al contenido de la auditoría.

IA Definitivo

- Elaboración del IA Definitivo: una vez cerrados los puntos abiertos o dudosos del IA Preliminar con el área auditada y con el Delegado de Protección de Datos u órganos de gobierno en materia de protección de datos, en su caso, el IA pasará al estadio de Definitivo.

- No conformidades en el IA Definitivo: en el caso de que persistan y no se hayan podido solventar con el auditor en la fase previa, podrán ser añadidas al final del IA Definitivo, encargándose el Delegado de Protección de Datos de recopilarlas formalmente entre las áreas o partes auditadas, ejerciéndose así el derecho de contradicción con el resultado final de la auditoría.

7.4. Plan de Acción

De acuerdo con la ISO 19011[15] , cuando exista un plan de acción de la auditoría, los participantes deben acordar el periodo de tiempo que trate los hallazgos de la auditoría. "El grado de detalle debería tener en cuenta la eficacia del sistema de gestión para alcanzar los objetivos del auditado, incluyendo consideraciones sobre su contexto y los riesgos y oportunidades". También es necesario acordar y establecer el seguimiento del plan de acción.

Las acciones pueden estar alineadas con estándares reconocidos, como la reciente ISO/IEC 27701:2019 *Security techniques — Extension to ISO/IEC 27001 y la ISO/IEC 27002 for privacy information management — Requirements and guidelines*[16], que se constituye en un sistema de gestión para proteger los datos personales. De esta manera, las acciones serán coherentes con los requerimientos, medidas y controles establecidos en normas y legislaciones, ya sean locales o internacionalmente reconocidas.

Siguiendo la *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD* de la AEPD se observa que en el apartado "5.4 Anexo IV: Plantilla de plan de acción y conclusión" se ofrece un modelo de plan de acción.

Dicho modelo contiene los aspectos básicos del plan para implantar y realizar el seguimiento de las medidas y garantías identificadas para gestionar el riesgo que, del mismo modo, puede servir como base para el plan de acción derivado de una auditoría RGPD.

En el mismo se han de detallar, como mínimo, los hallazgos o no conformidades detectados y que requieren de un plan de acción, las tareas, calendario previsto, los responsables de implantar y de supervisar y, en su caso, el riesgo vinculado al incumplimiento o la gravedad de la infracción asociada. Se han de establecer revisiones periódicas indicando el estado de las acciones.

A efectos de priorización de las medidas que han de detallarse en el plan de acción, se pueden tomar en consideración los indicadores descritos en el capítulo 6 de la presente Guía.

Cada compañía, en función de sus procesos, puede integrar los planes de acción en sus sistemas de gestión (de Riesgos, Seguridad, Privacidad, Compliance, etc.), añadiendo los campos que se consideren necesarios. De esta manera, el Plan de Acción abordará, entre otros, los siguientes aspectos:

[15] AENOR. UNE-EN ISO 19011:2018 Directrices para la auditoría de los sistemas de gestión. (ISO 19011:2018).
[16] International Organization for Standardization. ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

- Responsabilidad de las partes: Área auditada y/o Delegado de Protección de Datos u órganos de gobierno en materia de protección de datos personales.

- Se han de acordar las responsabilidades relacionadas con las acciones a desarrollar, teniendo en cuenta las establecidas en el RGPD, así como las que sean inherentes a la Organización que haya sido auditada.

- Forma de descripción de medidas. Las medidas se orientan al cumplimiento del RGPD, por lo tanto, los recursos que ofrece la AEPD son de gran ayuda para identificar el aspecto de cumplimiento al que se dirige la acción, así como el tipo de medidas que ayudarán a mitigar el riesgo: el "Listado de Cumplimiento Normativo" y la "Guía práctica de Análisis de riesgos en los tratamientos de datos personales sujetos al RGPD". Del mismo modo, si resultara viable, es recomendable incluir el presupuesto correspondiente a las medidas a adoptar en función del coste-esfuerzo-beneficio.

- Fechas de implantación. Ayudarán a evaluar el estado y grado de avance del plan. Permitirán a los responsables establecer las prioridades, dotar de recursos e implantar las acciones y que puedan tener una visión clara del riesgo en cada momento.

- Posibilidad de replanificación del plan/medidas. El seguimiento periódico de las medidas permitirá evaluar los grados de avance, así como la conveniencia o no de modificar plazos o ajustar las acciones en curso.

- Riesgos que puede asumir la organización en caso de que las no conformidades/incumplimientos no sean subsanados y esto sea detectado por una Autoridad de Control.

08

Reporte de resultados

Con la presentación de resultados concluye la fase final de la auditoría. Dicha presentación deberá realizarse con el fin de facilitar a los interlocutores y/o responsables de las áreas auditadas una clara comprensión de los resultados derivados de la auditoría para que, a partir de ellos promuevan el compromiso de aplicar, eficazmente, las acciones correctivas recogidas en el Informe final y la concienciación sobre el nivel de cumplimiento atribuible a la organización, con respecto a la normativa de protección de datos personales.

Por tanto, es necesario que dicha presentación sea precisa y convincente, teniendo en cuenta que los resultados aludidos en ella podrán ser utilizados por parte de la entidad auditada para acreditar el nivel de cumplimiento frente a terceros y como punto de referencia para futuras actividades de seguimiento.

8.1. Fase previa de la presentación de resultados

Antes de presentar los resultados al Responsable del tratamiento, conviene confirmar los siguientes aspectos:

- Que se han cumplido satisfactoriamente los objetivos, metas y alcances de la auditoría, siguiendo la metodología determinada en la fase inicial.
- Que los hallazgos y conclusiones recogidos en el informe se encuentran debidamente respaldados a partir de pruebas suficientes o evidencias objetivas.
- Que se ha remitido el Informe final a los interlocutores o representantes de la entidad auditada y que éstos han tenido oportunidad de revisar su contenido.
- Que no existe controversia, pendiente de ser solventada, con respecto a los hallazgos, observaciones y conclusiones que se recogen en el Informe final de auditoría, particularmente, en lo que concierne a las no conformidades detectadas.
- Que la valoración final del equipo auditor en cuanto al nivel de cumplimiento atribuible a la entidad, operación o sistema de información auditado, se fundamenta en criterios de razonabilidad y objetividad, generados a partir de un proceso sistemático y metódico.
- Que se han identificado a los interlocutores designados por el Responsable del Tratamiento a quienes se presentarán los resultados de la auditoría y que éstos tienen capacidad de decisión suficiente para asumir los resultados y acometer las medidas correctivas que pudieran derivarse de la misma (p.e. Delegado de protección de datos, alta dirección, responsables de áreas

auditadas u otras áreas de interés).

- Que se ha previsto una fecha, próxima a la emisión del Informe final, para realizar la reunión de cierre y presentación de resultados frente a los interlocutores identificados en el apartado anterior. La presentación de resultados no debería dilatarse excesivamente con respecto a la emisión del Informe final.

8.2. Presentación de resultados

Durante la reunión de cierre y presentación de resultados de la auditoría se realizará exposición analítica y depurada de los principales hallazgos, observaciones y conclusiones recogidos en el Informe final, destacando los aspectos más relevantes del trabajo realizado.

Resulta oportuno presentar los resultados de la auditoría con suficiente precisión y claridad, siguiendo un orden o estructura congruente con el Informe final, ya que, en cierta medida, la eficacia de los objetivos perseguidos con la auditoría, así como la ejecución de las acciones y compromisos derivadas de la misma, dependerán del discernimiento de tales resultados y conclusiones.

En función de la organización y el marco de gestión de Cumplimiento propio de la entidad auditada, los resultados de la auditoría se comunicarán a los correspondientes perfiles profesionales. En una primera fase, es recomendable que los resultados se comuniquen al Delegado de Protección de Datos o al área de Cumplimiento en caso de que no se haya nombrado un DPD. En caso de realizarse la auditoría por una entidad externa, los resultados asimismo se deberían comunicar al departamento de Auditoría Interna. En una fase posterior, los resultados se deberían comunicar a la alta dirección de la entidad, de nuevo, en función del marco organizativo de la entidad y los protocolos de gestión de cumplimiento implementados. Dicha comunicación puede bien realizarse por el Delegado de Protección de Datos, el área que impulsa la realización de la auditoría (por ejemplo: área de Compliance) o Auditoría Interna. En caso de una auditoría externa, previo acuerdo con el área interna del responsable del tratamiento que haya impulsado su realización, la comunicación a la alta dirección puede realizarse por la propia entidad externa.

Una vez presentados los resultados, convendría obtener una confirmación por parte de los interlocutores de la entidad auditada que asistieron a la reunión de cierre, a partir de la cual se manifieste que los resultados de la auditoría han sido conocidos, compren-

didos, contrastados y aceptados. Dicha confirmación podrá documentarse mediante la emisión de un "acta de la reunión de cierre y presentación de resultados de auditoría", o documento similar suscrito por los participantes de dicha reunión.

8.3. Seguimiento de las actividades pendientes

Resulta habitual que como consecuencia de la presentación de resultados de la auditoría se deriven compromisos y/o tareas a ser realizadas, posteriormente, por parte de la entidad auditada con el fin de subsanar las no conformidades residuales que hayan persistido tras el cierre de la auditoría. Tales compromisos y acciones correctivas surgen de las recomendaciones o acciones correctivas que el equipo auditor ha señalado en su Informe final.

Por lo tanto, se procurará acordar la manera en que la organización atenderá dichas recomendaciones o propuestas de mejor cumplimiento, estimando: la fecha de ejecución, quién será el responsable de llevarlas a cabo y quien será el responsable de verificar su seguimiento, ejecución o cierre de las actividades pendientes y cuando se realizará dicha verificación.

La designación de estas tareas podrá realizarse siguiendo la metodología RACI (Responsible, Accountable, Consulted, Informed), utilizada para la coordinación o gestión de proyectos a partir de los cuales se atribuyen responsabilidades a los diferentes actores que participan en la ejecución de las actividades que, en este caso, serían las que hayan quedado pendientes de subsanación tras el cierre de la auditoría.

Dicha metodología se representa mediante la creación de una matriz que se construye con una tabla en cuyas filas se incluirán las tareas determinadas, mientras que en sus columnas los actores designados (individuos o equipos de trabajo) para acometer dichas tareas.

Siguiendo la metodología RACI se establecerían las siguientes figuras de responsabilidad que corresponderían a cada tarea asignada:

METODOLOGÍA RACI

- **RESPONSIBLE (R) -** Responsable de ejecutar la acción correctiva o actividad para subsanar la no conformidad detectada en el informe de auditoría (por ejemplo: recurso, propio o externo, a quien se le haya asignado la ejecución de dicha tarea).

- **ACCOUNTABLE (A) -** Responsable de supervisar que dicha tarea se ejecute, sin necesidad de ser el que la ejecute y responsable de rendir cuentas sobre su ejecución (por ejemplo: director de la unidad de negocio, o responsable del área en la que se detectó la no conformidad).

- **CONSULTED (C) -** Figura que debe ser consultada para la realización de la tarea (por ejemplo: asesoría jurídica, consultor externo, privacy steward o designado de protección de datos, responsable de seguridad de la información).

- **INFORMED (I) -** Figura que debe ser informada sobre la realización de la tarea (por ejemplo: Delegado de Protección de datos, comité de auditoría).

El seguimiento o ejecución de estas actividades residuales deberá alinearse con los resultados de la auditoría, en el sentido en que para poder cerrar cada una de las tareas pendientes se habrá de confirmar que se hayan efectuado satisfactoriamente las acciones correctivas o recomendaciones para subsanar las no conformidades detectadas.

Asimismo, para el seguimiento de cada tarea/responsabilidad asignada, podrán acordarse: (i) fecha de compromiso de ejecución de la acción correctiva; (ii) fecha de seguimiento o comprobación de la ejecución de dicha tarea.

En este sentido, se definirán los responsables de atender estos compromisos, registrando los datos del seguimiento, las fechas específicas para verificar dicho seguimiento, junto con los cargos de los responsables de corroborar dicho seguimiento y los resultados de dicho ejercicio.

Finalmente, el seguimiento de las actividades pendientes, podrá integrarse dentro del ciclo de mejora continua o control interno implantado en la entidad, o bien podrá verificarse mediante una auditoría subsecuente o posterior que permitirá constatar los resultados del seguimiento y, en su caso, el cierre final de las actividades pendientes.

ANEXO I

Esquema de informe de Auditoría

isms forum

1. DATOS GENERALES

1.1. Los objetivos de la Auditoría

Se indicarán los objetivos de la auditoría como es la comprobación del grado de cumplimiento con la normativa objeto de auditoría, determinación de las incorrecciones o no conformidades respecto al cumplimiento de la misma y, en su caso, determinación de las acciones correctoras.

1.2. El alcance de la Auditoría, la normativa objeto de Auditoría, identificación de la organización auditada y de funciones o procesos auditados

Se indicarán, en primer lugar, la normativa objeto de revisión (RGPD, LOPDGDD, otras normativas locales etc.). Por otro lado, es necesario especificar los procesos, tratamientos, medidas o sistemas auditados, el rol que la entidad auditada asume en los mismos (responsable/encargado) así como la propia identificación de la/s sociedad/es auditada/s. Asimismo, se puede especificar la estructura de gobierno en materia de protección de datos existente en la entidad auditada.

1.3. La identificación del equipo auditor y de los participantes del auditado en la Auditoría

Se especificarán los miembros del equipo auditor con los respectivos roles que desempeñan (jefe de proyecto, auditor técnico, auditor jurídico-organizativo etc.) así como los participantes por parte de la entidad auditada (responsable del proyecto de la entidad, personas entrevistadas etc.)

1.4. Las fechas y ubicaciones donde se realizaron las actividades de Auditoría

Se indicará la duración de la auditoría y fechas específicas si fuese oportuno, así como las ubicaciones en las que se realizaron las actividades, tanto del auditado como del equipo auditor si procede.

2. METODOLOGÍA DE AUDITORÍA

Es necesario exponer la metodología empleada para el desarrollo de la auditoría. La misma puede basarse en un estándar reconocido o en la metodología propia del auditado o la entidad auditora. En cualquier caso, se recomienda hacer hincapié en la valoración de las evidencias y, en su caso, en la metodología empleada para la valoración y/o cálculo

del grado de cumplimiento con la normativa objeto de auditoría.

3. HALLAZGOS Y EVIDENCIAS RELACIONADAS

Se expondrán los hallazgos de la auditoría con el grado de detalle necesario. Se recomienda dividir los hallazgos conforme a los correspondientes dominios funcionales auditados (Información y consentimiento, Derechos de los Interesados etc.). Respecto a cada dominio funcional, es recomendable incluir un apartado de referencias normativas a fin de vincular el mismo con las obligaciones auditadas. Las evidencias relacionadas con los dominios funcionales pueden bien incorporarse en los correspondientes apartados de cada dominio o incluirse a modo de anexo como una relación de las evidencias consideradas por el auditor. Por otro lado, y sin perjuicio de la elaboración del plan de acción, respecto a cada hallazgo o no conformidad pueden indicarse las acciones correctoras necesarias para subsanar la misma.

4. EVALUACIÓN DEL GRADO DE CUMPLIMIENTO

En relación con los hallazgos identificados en el apartado anterior del informe, se recomienda especificar el grado de cumplimiento de la organización respecto a la normativa objeto de auditoría. Sujeto a la metodología empleada para la realización de la auditoría, se podrán especificar los grados de cumplimiento globales (por cada responsable del tratamiento o a nivel grupo si la auditoría ha comprendido varias empresas del mismo grupo empresarial), por dominio funcional u otros en función de las métricas e indicadores de los que dispone el auditor (p.ej. grado de implementación de controles, eficacia de los mismos etc.).

5. CONCLUSIONES DE LA AUDITORÍA

El capítulo de conclusiones de la auditoría debería incluir a modo de resumen los hallazgos y resultados de la auditoría. Se recomienda la incorporación de gráficos relativos a los resultados de la auditoría como representación visual de la información obtenida. Asimismo, las conclusiones se pueden acompañar con información que permita completar la valoración del riesgo por parte del Delegado de Protección de Datos u órgano de gobierno en materia de protección de datos.

6. CONTENIDO OPCIONAL

6.1. Resumen ejecutivo

En relación con la fase de comunicación de los resultados de la auditoría y con el objetivo de facilitar la revisión del informe, se puede incorporar un resumen ejecutivo de los hallazgos de la auditoría bien al principio del informe o al final del mismo.

6.2. Cualquier opinión divergente sin resolver entre el equipo auditor y el auditado

Si bien se recomienda que los auditores consensuen el contenido del informe con la entidad auditada, es posible que queden ciertas discrepancias entre éstos respecto a alguno de los aspectos del informe de auditoría. En este sentido, se pueden incluir dichas opiniones divergentes en el informe de auditoría.

6.3. Indicaciones relacionadas con el riesgo derivado del muestreo

Es habitual que la revisión de las evidencias se realice mediante un muestreo debido al volumen de las mismas (p.ej. contratos con encargados del tratamiento). Por tanto, es recomendable que se incluya un apartado describiendo la metodología de muestreo empleada y las posibles consecuencias de la misma.

6.4. Confirmación sobre el cumplimiento de los objetivos de la Auditoría en el marco del plan de Auditoría de la entidad

Si la entidad dispone de un plan de auditoría, el informe puede contemplar un apartado que vincula los objetivos que persigue la auditoría realizada y los resultados de la misma con dicho plan.

6.5. Cualquier área dentro del alcance de la Auditoría no cubierta

Si no se ha podido realizar la auditoría en algún aspecto incluido el planteado alcance, se debería reflejar lo mismo en el informe, incluyendo cualquier cuestión sobre la disponibilidad de las evidencias, los recursos o la confidencialidad, con las justificaciones relacionadas.

6.6. Buenas prácticas identificadas y mejora continua

Si en el curso de la auditoría se ha identificado que la entidad gestiona cierto proceso o tratamiento con unas buenas prácticas, el informe puede reflejar este hecho. Del mismo modo, si la entidad ha sido previamente sujeta a auditorías RGPD, se pueden vincular los resultados de las auditorías anteriores con los hallazgos de la auditoría realizada en línea con el ciclo de mejora continua.

6.7. Recomendaciones de mejora del auditor

Sin perjuicio de las acciones correctoras que se incluirán en el plan de acción, los auditores pueden realizar recomendaciones de mejora respecto a aquellos hallazgos que no llegan a constituir una no conformidad.

6.8. Seguimiento acordado del plan de acción

Si se ha acordado la participación de los auditores en las actividades del seguimiento del plan de acción, se puede incorporar en el informe de auditoría el modelo de seguimiento acordado para tal fin.

6.9. Declaración sobre la naturaleza confidencial de los contenidos

Es habitual que los informes de auditoría incorporen información confidencial de la entidad auditada y, en caso de auditorías externas, información confidencial o know-how de la entidad auditora. En este caso, será preciso elaborar un disclaimer relativo al uso de dicho informe y los supuestos en los que se permitirá su revelación a terceros.

Más información en:
www.ismsforum.es

 @ISMSForum

 ISMS Forum

isms forum

INTERNATIONAL
INFORMATION
SECURITY
COMMUNITY