CAPÍTULO 3
LA AUDITORÍA. CONCEPTO Y CARACTERÍSTICAS

1. CONCEPTO

La palabra auditoría viene del latín *auditorius,* y la Real Academia Española de la Lengua la define como:

> *Revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a las que aquellas deben someterse.*

Para el tema que nos ocupa, que es la verificación de la protección de datos en las empresas expondremos otra definición de auditoría. Se entiende por **auditoría** a la investigación, consulta, revisión, verificación, comprobación y obtención de la evidencia sobre un hecho acontecido o sistema establecido, según el desarrollo de las normas de aplicación, a través de la certificación de personal cualificado y acreditado al respecto.

Es un proceso sistemático, esto quiere decir que en toda auditoría debe existir un conjunto de procedimientos lógicos y organizados que el auditor debe cumplir para la recopilación de la información que necesita para emitir su opinión final sobre la adecuación de dicha empresa a la protección de datos.

También en esta definición se indica que la evidencia debe obtenerse y evaluarse de manera objetiva, esto quiere decir que el auditor debe realizar su trabajo con una actitud de independencia neutral frente a él.

La evidencia que debe obtener el auditor consiste en una amplia gama de información y datos que le puedan ayudar a elaborar su informe final. Esta defini-

ción no es estricta en cuanto a la naturaleza de la evidencia que se ha revisado, más bien nos indica que el auditor debe usar su criterio profesional para saber cuál de todas las evidencias que posee es la apropiada para el trabajo que está ejecutando, él debe considerar cualquier elemento o dato que le permita realizar una evaluación objetiva y expresar un dictamen profesional.

El auditor tiene un papel que desarrollar en este proceso, el cual es, determinar el grado de precisión que existe entre los hechos que ocurren en realidad y los informes que se han elaborado después de haber sucedido tales hechos.

Por último tendríamos que decir que la auditoría es una herramienta de control y supervisión que permite descubrir fallos en las estructuras o vulnerabilidades existentes en la organización de una empresa en materia de protección de datos.

2. Características fundamentales de la auditoría

Imparcialidad y objetividad

La actividad auditora deberá llevarse a cabo con objetividad e imparcialidad aunque la conclusión final de la misma es una opinión, esta debe basarse siempre en evidencias objetivas, es decir, debe tenerse en cuenta la información cuya veracidad pueda ser probada, basada en hechos, conocidos a través de la observación, medición, ensayo u otros medios, para poder comprobar la adecuación de la protección de datos en dicha empresa.

La actividad del auditor debe ejecutarse manteniendo independencia de criterio y decisión y no dejarse influenciar por factores externos o internos, de tal manera que siempre mantenga su criterio de independencia frente a la entidad o empresa que va a auditar, su actuación siempre debe estar fundada en la realidad de los hechos y demás circunstancias vinculadas a los mismos (actos, situaciones, evidencias), que le permitan mantener sobre bases sólidas sus juicios y opiniones sin deformaciones por subordinación a condiciones particulares.

Sistematización

Con el objeto de asegurar la uniformidad en la aplicación y dirección de trabajo, la auditoría debería desarrollarse mediante un proceso sistemático que implicaría la aplicación de una metodología, y por lo tanto, del uso de estándares, por ello la entidad auditora debería elaborar sus propios procedimientos y protocolos de actuación, dado que es ella la que mejor conoce sus posibilidades y recursos.

Documentación

El aspecto documental es de gran importancia en la auditoría de protección de datos, pues constituyen siempre la prueba más objetiva de que aquello que se

dice es cierto, ya que las pruebas documentales permiten evidenciar los hechos alegados.

La auditoría de protección de datos, se centra en los documentos que suministra el propio auditado, de hecho el proceso auditor gira básicamente en torno al denominado Documento de Seguridad (donde se refleja de alguna manera, toda la información en materia de protección de datos).También tienen gran relevancia otros elementos documentales, como los registros, que permiten evaluar la eficacia diaria del Sistema de Seguridad.

PERIODICIDAD

La periodicidad mínima con la que se ha de realizar una auditoría del sistema de información e instalaciones de tratamiento y almacenamiento de datos de carácter general es de 2 años según el RDLOPD en su Art.96.1. Aunque con el nuevo reglamento, se introduce la obligatoriedad de auditar antes de vencer el plazo de los 2 años, cuando se realicen modificaciones sustanciales en el sistema que puedan afectar a la seguridad de los datos.

3. Tipos de auditoría

Las auditorías pueden clasificarse en Externas e Internas.

Auditoría Externa

La auditoría externa, es el examen crítico, sistemático y detallado de un sistema de información, realizado por un profesional en la materia sin vínculos laborales con la empresa auditada, utilizando técnicas determinadas, destinadas a la revisión de los métodos de control o de seguridad empleados, para la protección de los datos de carácter personal, con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento.

En la auditoría externa la relación es de tipo civil, entre el auditor y la empresa auditada, mediante la realización de un contrato de prestación de servicios, como es el que le presentamos a continuación.

MODELO DE CONTRATO DE AUDITORÍA

En..., a... de... de 20...

REUNIDOS

De una parte..., con CIF..., como Responsable del/de los Fichero/s o Tratamiento/s, en adelante «el Auditado».

Y de otra..., en nombre y representación de..., domiciliada en... y CIF..., en adelante «los Auditores».

EXPONEN

1. Que el Auditado desea celebrar un contrato de auditoría de seguridad de protección de datos para dar cumplimiento a lo dispuesto en los artículos 96 y 110 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (R-DLOPD en adelante).
2. Que los Auditores están capacitados para el desempeño de la citada auditoría y aceptan el encargo.
3. Que a los fines indicados, ambas partes suscriben el presente contrato de auditoría de seguridad de protección de datos, que se regirá por las siguientes

CLÁUSULAS

PRIMERA. Los auditores realizarán la auditoría, con periodicidad bienal, de la empresa…Al completar la auditoría, emitirán un informe que contendrá su opinión técnica sobre los sistemas de información y el tratamiento de los datos de carácter personal de la empresa auditada.

Adicionalmente, los auditores informarán al Responsable de Seguridad sobre las debilidades significativas que, en su caso, hubieran identificado en la evaluación del control interno.

SEGUNDA. Los Auditores realizarán la auditoría de los sistemas de la información e instalaciones de tratamiento y almacenamiento de datos de carácter personal del Auditado, para verificar el cumplimiento del RDLOPD, así como de los procedimientos e instrucciones vigentes en materia de seguridad de datos.

Como parte de la auditoría, y únicamente a efectos de determinar la naturaleza, oportunidad y amplitud de los procedimientos de auditoría, los auditores tendrán en cuenta el funcionamiento interno de la EMPRESA. Además, el objetivo del trabajo de los Auditores es obtener una seguridad razonable de que los sistemas de la información e instalaciones de tratamiento y almacenamiento de datos de carácter personal de la Auditada estén libres de deficiencias significativas.

Sin embargo, dado que el examen de los auditores está basado principalmente en pruebas selectivas, estos no pueden garantizar que se detecten todo tipo de errores o irregularidades, en caso de existir.

Los papeles de trabajo preparados en relación con la auditoría son propiedad de los auditores, constituyen información confidencial, y estos los mantendrán en su poder de acuerdo con las exigencias de la LOPD. Asimismo, y de acuerdo con el deber de secreto establecido en dicha normativa, los auditores se comprometen a mantener estricta confidencialidad sobre la información de la entidad obtenida en la realización del trabajo de auditoría.

Por otra parte, los auditores en la realización de su trabajo mantendrán siempre una situación de independencia y objetividad.

TERCERA. Para la prestación del servicio de auditoría al responsable del fichero…, la organización…, acorde con los artículos 20, 21 y 22 del RDLOPD y el artículo 12 de la LOPD, establece que los datos personales a los que haya tenido acceso por la prestación de este servicio no serán considerados cesión de datos el acceso a los datos de carácter personal del cliente y solo los obtenidos en el marco de este contrato pasarán a un fichero denominado…, inscrito en la AEPD con la única finalidad de la prestación del servicio de auditoría. Se establece expresamente que la organización…, únicamente tratará los datos conforme a las instrucciones del cliente, expresadas en el presente Contrato, que no los aplicará o utilizará con fin distinto al que figura en lo pactado entre las Partes, ni los comunicará, ni siquiera para su conservación, a otras personas.
LA EMPRESA se compromete a adoptar e implantar las medidas técnicas y organizativas de seguridad a que se refiere el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y, en particular, las correspondientes al nivel básico establecidas en el Real Decreto 1720/2007, de 21 de diciembre, para los datos y ficheros objeto de este documento. Pueden ejercitar sus derechos de acceso, rectificación, oposición y cancelación acorde a como establece la normativa vigente de protección de datos en la siguiente dirección:

C/
CP
Ciudad

Una vez finalizado el objeto del contrato, la organización… se compromete a devolver todos aquellos materiales del cliente… o a destruirlos presentando un escrito que certifica la destrucción de materiales por parte de la organización…, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

CUARTA. El Auditado es responsable de la redacción de las medidas de seguridad, a través del Documento de Seguridad, así como de implantarlas en todos los niveles jerárquicos de la organización. El Auditado es también responsable de proporcionar a los Auditores, cuando éstos así lo soliciten, toda la documentación y registros de los ficheros y tratamientos auditados y la información relativa a los mismos, así como de indicar al personal a quién puedan dirigir sus consultas.

QUINTA. Los Auditores harán cuestiones específicas a los responsables y a los usuarios de los sistemas de la información e instalaciones de tratamiento de datos de carácter personal sobre la información contenida en el Documento de Seguridad y sobre la eficacia de su implantación.

SEXTA. La duración del presente contrato será de..., a contar desde el momento de aceptación por las partes.

SÉPTIMA. Los honorarios profesionales que deberán percibir los Auditores por el desempeño de su función serán de... Euros tomando en consideración el tiempo estimado necesario, y los conocimientos y experiencia profesional del personal asignado para la realización del encargo.

Si durante la realización del trabajo observaran los Auditores cambios en las circunstancias a partir de las cuales se ha realizado el presente contrato, tales como variación del número de centros de trabajo, del número de usuarios del sistema o de la organización de los sistemas de la información, se lo notificarán al Auditado, explicando los motivos que les obligan a modificar los honorarios estimados, a partir del número de horas que realizar en virtud de los cambios operados.
Para cada una de las auditorías sucesivas sujetas al presente contrato los honorarios tendrán como base el importe total señalado para la primera auditoría, al que se aplicará el incremento experimentado por el IPC del sector servicios.
Esta estimación tendrá validez siempre que no se modifiquen las circunstancias actuales en base a las cuales se ha realizado el presente contrato.
A los honorarios se les aplicará el IVA al tipo que se encuentre vigente.
Independientemente de los honorarios, los Auditores percibirán los suplidos que, como gastos necesarios, hayan tenido que realizar para el desempeño de su función.

OCTAVA. Los honorarios profesionales a percibir por los Auditores durante cada ejercicio serán abonados por el Auditado de la forma siguiente:
...% A la aceptación del encargo.
...% …
...% A la entrega del informe.

NOVENA – El presente contrato tiene por objeto exclusivo la realización de la auditoría de los sistemas de la información e instalaciones de tratamiento y almacenamiento de datos de carácter personal del Auditado en los términos previstos en la legislación vigente, quedando excluida del mismo cualquier otra actuación profesional que se encomiende por el Auditado a los Auditores.
Y en prueba de conformidad con cuanto antecede, ambas partes firman el presente contrato por duplicado en el lugar y fecha arriba indicados.

Fdo: Fdo:

Auditoría Interna

La auditoría interna es el examen crítico, sistemático y detallado de un sistema de información, realizado por una persona con conocimientos específicos sobre dicha materia que además debe ser abogado en ejercicio o ingeniero informático y que posea un vínculo laboral con la empresa, utilizando técnicas determinadas destinadas a la revisión de los métodos de control o de seguridad empleados para llevar a cabo la implantación de la LOPD en sus empresas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la misma. Estos informes son de circulación interna.

Las funciones de la auditoría son:

- Evaluar de forma permanente el funcionamiento de los controles internos establecidos por las empresas y recomendar las medidas que signifiquen mejorar su efectividad. Lo anterior puede derivar en una evaluación general del sistema de control interno y/o áreas específicas e incluso de aspectos constitutivos del control, como la organización, los procedimientos, los métodos, los sistemas de información y el personal.
- Verificar la existencia de adecuados sistemas de información, registro y control que generen resultados oportunos y veraces.
- Establecer el grado de implementación de las medidas preventivas y/o correctivas provenientes de las evaluaciones realizadas.
- Desarrollar las funciones de supervisión de todos los pasos realizados para llevar a cabo la implantación de la Ley Orgánica de la Protección de Datos de acuerdo con la normativa vigente y elaborar los informes relativos al estado de dicha implantación en la misma.

4. PERFIL DEL AUDITOR

Las auditorías deben llevarse a cabo por personas cualificadas de la misma organización que reúnan los requisitos necesarios o por Auditores externos que estén capacitados para ello, tanto legalmente como profesionalmente.

Ante esta situación cuando nos preguntamos qué perfil debe tener el auditor, debemos decir que la Agencia Española de Protección de Datos todavía no se ha pronunciado al respecto pero sí organismos privados como el INTECO (National Institute of Communication Technologies) o la norma de calidad ISO, en cuyos estándares podemos encontrar los requisitos básicos de un auditor, los cuales se exponen a continuación.

4.1. FORMACIÓN Y CAPACIDAD PROFESIONAL

El auditor debe ser un profesional colegiado, de forma que además de aportar la garantía del seguro de responsabilidad civil del profesional tenga la visión práctica del ejercicio profesional en el asesoramiento a empresas, de alguna de estas dos especialidades:

- Abogado en ejercicio, al tener que realizar el auditor la labor de interpretar normas administrativas complejas, así como interpretar contratos y documentos de contenido jurídico, siendo el informe jurídico una actividad restringida a los abogados conforme al estatuto de la abogacía.
- Ingeniero informático, dado que se debe realizar un análisis de los sistemas informáticos de la empresa o entidad.
- Tener una formación especializada en protección de datos, acreditada mediante la titulación de postgrado, master o curso avanzado, impartidos por universidad o entidad reconocida de prestigio.
- Conocimientos técnicos básicos de estructura de red, aportando experiencia en el asesoramiento o consultoría en ese campo o conocimiento teórico mediante cursos de formación.

- Se podría valorar también para un mayor nivel de exigencia, el conocimiento de cuestiones en materia de firma digital, cifrada de documentos, etc.

4.2. Independencia, integridad y Objetividad

El auditor durante su actuación profesional deberá mantener una posición de absoluta independencia, integridad y objetividad. La independencia supone una actitud mental que permite al auditor actuar con libertad respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad en la consideración objetiva de los hechos, así como en la formulación de sus conclusiones. La integridad debe entenderse como la rectitud intachable en el ejercicio profesional, que le obliga, en el ejercicio de su profesión, a ser honesto y sincero en la realización de su trabajo y en la emisión de su informe. En consecuencia, todas y cada una de las funciones que ha de realizar han de estar presididas por una honradez profesional irreprochable. La objetividad implica el mantenimiento de una actitud imparcial en todas las funciones del auditor, para ello deberá gozar de una total independencia en sus relaciones con la entidad auditada. Debe ser justo y no permitir ningún tipo de influencia o prejuicio.

Para ser independiente el auditor no debe tener intereses ajenos a los profesionales, ni estar sujeto a influencias susceptibles de comprometer tanto la solución objetiva de los problemas que puedan serle sometidos, como la libertad de expresar su opinión profesional. El auditor debe ser siempre independiente y abstenerse de aceptar el encargo de auditoría en todos aquellos casos en que incurra en una situación incompatible con el ejercicio de sus funciones.

4.3. Diligencia Profesional

El auditor en la ejecución de su trabajo y en la emisión de su informe actuará con la debida diligencia profesional. La debida diligencia profesional impone a cada persona de la organización del auditor, la responsabilidad del cumplimiento de las Normas en la ejecución del trabajo y en la emisión del informe. Su ejercicio exige, asimismo, una revisión crítica a cada nivel de supervisión del trabajo efectuado y del juicio emitido por todos y cada uno de los profesionales del equipo de trabajo de auditoría. El auditor debe aceptar únicamente los trabajos que pueda

efectuar con la debida diligencia profesional. El auditor debe demostrar su diligencia profesional en los papeles de trabajo, lo cual requiere que su contenido sea suficiente para suministrar el soporte de opinión.

4.4. RESPONSABILIDAD DEL AUDITOR

El auditor es responsable del cumplimiento de las normas de auditoría establecidas, y a su vez responsable del cumplimiento de las mismas por parte de los profesionales de su equipo de auditoría. Las responsabilidades y actividades del auditor son:

- Planear y desarrollar las tareas asignadas, objetiva, efectiva y eficientemente.
- Recopilar y analizar las evidencias de auditorías relevantes y suficientes para determinar los resultados de la auditoría.
- Preparar los documentos de trabajo.
- Documentar los resultados individuales de la auditoría.
- La redacción del informe de auditoría.

4.5. SECRETO PROFESIONAL

El auditor debe mantener la confidencialidad de la información obtenida en el curso de sus actuaciones. El auditor ha de mantener estricta confidencialidad sobre toda la información adquirida en el transcurso de la auditoría concerniente a la protección de datos, excepto en los casos previstos en la Ley, no revelará el contenido de la misma a persona alguna sin autorización del cliente. No obstante, el auditor deberá recoger en su informe cualquier negativa del cliente a mostrar toda la información necesaria para expresar la imagen fiel de sus actividades. El auditor tiene, asimismo, el deber de garantizar el secreto profesional en las actuaciones de sus ayudantes y colaboradores. La información obtenida en el transcurso de sus actividades de auditoría no podrá ser utilizada en su provecho ni en el de terceras personas.

La auditoría podrá realizarse por una sola persona (auditor), o por un grupo de personas cualificadas en la materia conocido como Equipo Auditor, del que a

continuación estableceremos su organización, funciones y responsabilidades en materia de protección de datos.

6. Equipo Auditor

El Equipo Auditor está formado por el auditor líder y demás miembros del equipo, quienes pueden ser auditores o expertos técnicos.

Para asegurar la objetividad del proceso de auditoría, sus resultados y cualquier conclusión, los miembros del equipo auditor deben ser independientes de las actividades que auditan, deben ser objetivos, y libres de tendencia o conflicto de intereses durante el proceso.

El uso de miembros externos o internos del equipo auditor está sujeto a discreción del cliente. Un miembro del equipo auditor escogido dentro de la organización no debe ser responsable directamente del tema que se está auditando.

Los miembros del equipo auditor deben poseer una combinación apropiada de conocimientos, habilidades y experiencias para cumplir con las responsabilidades de la auditoría.

Los miembros del equipo auditor serán los siguientes:

- **Auditor jefe**

  El auditor líder es el responsable de asegurar una conducta eficiente y efectiva de la auditoría dentro de los alcances de la misma.

  Adicionalmente, el auditor jefe tiene las siguientes responsabilidades y actividades que cumplir:

- Consultar y consensuar con el cliente el alcance de la auditoría.
- Obtener la información o documentación necesarias para conocer las actividades de la empresa.
- Formación del equipo auditor y asignación de tareas específicas, o actividades por auditar a los mismos.
- Dirigir las actividades del equipo auditor.
- Preparar las comunicaciones.
- Coordinar la preparación de los documentos y procedimientos detallados de trabajo y reunir al equipo auditor.
- Representar al equipo auditor en discusiones con el auditado, antes, durante y después de la auditoría.
- Realizar los informes de la auditoría para el cliente.

- **De los auditores**

  Los auditores integrantes de los equipos de auditoría, trabajan bajo la supervisión directa del jefe de equipo y sus principales funciones son las siguientes:

  - Aplicar los programas de auditoría preparados para el desarrollo del trabajo, conforme a las instrucciones del jefe de equipo.
  - Documentar la aplicación de los procedimientos de auditoría utilizando la estructura y orden definido para los papeles de trabajo.
  - Cumplir con los criterios de ejecución establecidos para su trabajo, así como, los estándares profesionales (normas de auditoría) y

encontrar dificultades, comunicarlas de inmediato al auditor jefe de equipo de la auditoría.

- Mantener ordenados y completos los papeles de trabajo.
- Sugerir procedimientos alternativos o adicionales para promover la eficiencia en las actividades de auditoría realizadas.
- Colaborar continuamente para fomentar el logro de los objetivos incluidos en la planificación específica.
- Obtener la evidencia suficiente, competente y pertinente de los hallazgos de auditoría, desarrollar sus principales atributos y analizarlos con el jefe de equipo de la auditoría.
- Redactar, en la correspondiente cédula o papel de trabajo, los resultados del examen, (comentarios, conclusiones y recomendaciones) sobre cada componente desarrollado, guiándose con la estructura preestablecida para el informe final.
- Estructurar el expediente de papeles de trabajo y entregarlo al jefe de equipo para la integración completa de los resultados y su correspondiente archivo.
- Cumplir con las disposiciones legales, normatividad e instrucciones relacionadas con el ejercicio de la auditoría, así como observar el Código de Ética Profesional.

En definitiva las responsabilidades de los auditores de una forma resumida serían las siguientes:

RESPONSABILIDADES DE LOS AUDITORES
• Cumplir con los requisitos de auditoria aplicables. • Comunicar y aclarar los resultados de auditoria. • Planificar y realizar las responsabilidades asignadas de forma eficaz y eficiente. • Documentar las observaciones. • Redactar informes con los resultados de auditorias. • Verificar la eficacia de acciones correctivas. • Retener y guardar los documentos de auditoria: - Presentar dichos documentos de la forma requerida. - Asegurarse que dichos documentos sean confidenciales. - Tratar la información confidencial con discreción. • Cooperar con el auditor jefe y apoyarle.

- **Responsabilidades del cliente y auditado**

  Las responsabilidades deben:

  – Definir los objetivos de la auditoría.
  – Proveer de los recursos necesarios al auditor para conducir la auditoría.
  – Aprobar el plan de auditoría.
  – Recibir el informe de la auditoría y determinar su distribución.
  – Informar a los empleados de los objetivos y alcance de la auditoría, cuando sea necesario.
  – Designar personal responsable y competente para acompañar a los miembros del equipo auditor, para actuar como guías dentro de la empresa y para asegurar que los auditores puedan realizar el desempeño de su labor.
  – Proveer el acceso a las instalaciones, personal, información y registros relevantes a solicitud de los auditores.

1. ¿Cuáles son las características fundamentales de una auditoría?

2. ¿Qué condiciones y comportamientos debe reunir el auditor para el desarrollo de la actividad auditora?

3. Mencione las responsabilidades y actividades que debe cumplir el auditor jefe.

Ejercicios de Repaso y Autoevaluación