La privacidad de los datos y la auditoría

Author : gochoadealda

Categories : Auditoría, Certificación y Calidad de Sistemas Informáticos

Date : 1 diciembre, 2018

En este post se hablará de la auditoria respecto a la privacidad de los datos y más concretamente respecto de la RGPD.
La visión de la RGPD sobre la auditoría va muy ligada a la labor del DPD (delegado de protección de datos) y al análisis de riesgos e impacto, ambos temas han sido tratados en post anteriores. A pesar de dejar claras las líneas generales, no se determina claramente cuál es la función del DPD sobre la auditoría, si no que más bien se recomienda establecer una figura como el DPD, en caso de no haber DPD, que lleve acabo las funciones del mismo y que además supervise el análisis de riesgos. Si se establece que, aunque la labor del DPD este relacionada con procesos de supervisión ligados a temas de auditoría, en algunos casos, no es la labor del DPD realizar la auditoría.
Pero antes de meternos en materia vamos a empezar por el principio, ¿Qué es la auditoría? ¿Que es auditar?
La auditoría es un proceso sistemático, independiente y documentado mediante el cual se busca obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen unos criterios previamente establecidos. Estos criterios se basan en estándares, leyes o normativas que aquello que auditamos o aquello a lo que sometemos al proceso de auditoría debe cumplir.
La finalidad de la auditoría puede ser completamente definida, buscando un objetivo muy concreto, o referirse a más de un objetivo, siendo más general. Lo habitual es querer conocer las debilidades e incumplimientos, puede hacerse también como garantía de que una entidad está cumpliendo con los requisitos establecidos o con lo que se haya comprometido a cumplir y así disminuir riesgos. También se puede dar el caso de que lo exijan sus clientes, o que sin una exigencia específica la entidad quiera tener un informe que, en caso de ser favorable, constituya una ventaja comercial.
Según el objetivo podemos basarnos en diferentes fuentes de información para llevar a cabo la auditoría, en el caso de la protección de datos se sugiere la ISO 27001, que se basa en la protección de la información y en los propios datos de carácter personal. Ambas normativas se consideran complementarias (RGPD e ISO 27001). [1]
La profundidad mínima será la que permita alcanzar evidencias para sustentar los informes requeridos, puede ser suficiente mediante entrevistas, análisis y muestreos, pero en ocasiones se requiere verificar los perfiles de todos los usuarios, el seguimiento de todas las incidencias, investigar hechos anteriores, etc.
Hay cuatro artículos concretos de la RGPD en los que se hace referencia a la auditoría:

- **Artículo 28**, Encargado del tratamiento: punto 3 en el apartado h): “Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para

permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable". [2]

- **Artículo 39**, Funciones del delegado de protección de datos (DTD): entre ellas: "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". [3]
- **Artículo 47**, Normas corporativas vinculantes: entre ellas: "los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado". [4]
- **Artículo 58**, Poderes: referido a los de "cada autoridad de control", definido entre los poderes de investigación: "llevar a cabo investigaciones en forma de auditorías de protección de datos, que en el caso de las autoridades de control en España puede que establezcan como inspecciones, que con frecuencia asociamos con posibles sanciones". [5]

Además, es importante hablar de diferentes tipos de auditoría que podemos realizar o la que las entidades se pueden someter en este ámbito.

- Auditoría interna: Control interno que realiza la empresa para supervisar determinados procesos o evaluar el funcionamiento de la misma.
- Auditoría externa: Una empresa externa es la encargada de realizar la auditoría a la entidad.
- Auditoría de seguridad: se basa en la verificación del análisis de riesgos que haya llevado acabo la entidad, y la valoración de las amenazas existentes y controles implantados, para determinar la vulnerabilidad y la gestión del impacto que estas vulnerabilidades puedan tener.
- Auditoría de cumplimiento: suele abarcar muchos aspectos jurídicos, es la parte más técnica, se refiere a la verificación del correcto cumplimiento de las normativas y leyes.

Espero que este post haya sido de ayuda de cara a introducirnos en el ámbito de la auditoría en el campo de la privacidad y protección de los datos, especialmente en lo referente a la RGPD.

Referencias

[1]Fundamentos de iso 27001 y su aplicación en las empresas
[2] http://www.privacy-regulation.eu/es/28.htm
[3] http://www.privacy-regulation.eu/es/39.htm

[4] http://www.privacy-regulation.eu/es/47.htm
[5] http://www.privacy-regulation.eu/es/58.htm
https://www.sage.com/es-es/blog/rgpd-como-hacer-una-auditoria-en-tu-empresa-antes-de-su-entrada-en-vigor/
http://www.iee.es/pages/bases/articulos/prodaud.html