TEST DE REFLEXIÓN: LA PROTECCIÓN DE LOS DATOS Y EL COMERCIO ELECTRÓNICO

Es muy importante que se identifiquen todas aquellas cuestiones que pueden afectar a los resultados actuales o futuros. Para ello se debe analizar cada uno de los 40 ítems o preguntas y asignar la respuesta que mejor define la realidad que está viviendo la empresa. Este análisis puede ser más completo si intervienen las personas que conocen el significado y la situación de los distintos ítems. Para cada uno de ellos sólo existen 3 respuestas posibles:

- ***SI.*** *Ocurre lo descrito en la pregunta en sus propios términos.*
- ***NO.*** *En la empresa no sucede lo que se describe en la pregunta. Es una situación negativa y conlleva una necesidad de actuar.*
- ***N/A (No Aplica).*** *Cuando el tema detallado no se aplica, es decir no es de la incumbencia de la empresa, o no le afecta.*

*Se puntuará como **NO**, tanto cuando la circunstancia descrita no sucede en la empresa, como, cuando acaeciendo, se da en unas condiciones mediocres o muy mejorables.*

Marque, por favor, la casilla de la respuesta que más se asemeja a la realidad de su empresa.

1.- ¿Es consciente la empresa de que dispone de datos de carácter personal de empleados, clientes o proveedores y está obligada al cumplimiento de la LOPD?

SI NO N/A

2.- ¿Conoce la empresa con exactitud cuáles son los datos personales que están afectados por esta ley y cuáles no?

SI NO N/A

3.- ¿Ha adoptado la compañía las medidas de seguridad técnicas y administrativas adecuadas para la protección de datos de personas físicas, en cumplimiento de la citada ley?

SI NO N/A

4.- ¿Posee los escritos de la Agencia Española de Protección de Datos (AEPD) donde se otorga el número de inscripción en el registro de los ficheros?

SI NO N/A

5.- ¿Tiene elaborado adecuadamente el documento de seguridad interno y ha implementado las medidas y procedimientos para su correcta aplicación?

SI NO N/A

6.- ¿Dicho documento de seguridad es revisado periódicamente por el responsable asignado a ello?

SI NO N/A

7.- ¿Dispone de los oportunos contratos de los encargados de tratamiento?

SI NO N/A

8.- ¿La empresa trata los datos de la persona a la que pertenecen con su consentimiento o bien sin el mismo porque existe una Ley o una relación negocial que se lo permite?

SI NO N/A

9.- ¿En el proceso de obtención de los datos, la compañía informa a la persona a la que pertenecen de los aspectos básicos de protección de datos?

SI NO N/A

10.- ¿En cuanto a los datos, únicamente los rectifica o cancela cuando se lo solicita un interesado, no disponiendo de ningún método de actualización?

SI NO N/A

11.- ¿La empresa ha dado instrucciones precisas para que los trabajadores y colaboradores relacionados con el tratamiento guarden el debido secreto y confidencialidad?

SI NO N/A

12.- ¿La compañía conoce los derechos que la LOPD otorga a las personas cuyos datos trata?

SI NO N/A

13.- ¿Se han establecido los procedimientos para facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación?

SI NO N/A

14.- ¿Sabría la compañía como actuar si alguien le solicita acceder a sus datos personales o bien rectificarlos o cancelarlos?

SI NO N/A

15.- ¿Los formularios donde los clientes solicitan los servicios o productos de la empresa, contienen cláusulas respetando el derecho a la privacidad de los datos que le son entregados?

SI NO N/A

16.- ¿Tiene la empresa contratada algún servicio con terceros mediante el cual le gestiona los datos de carácter personal de los que la compañía es propietaria (gestión de nóminas, de la contabilidad, facturación, etc.)?

SI NO N/A

17.- ¿Es consciente la compañía que infringir la L.O.P.D., puede suponer sanciones de entre 600 y 600.000 euros?

SI NO N/A

18.- ¿Se conoce en la empresa que algunos datos personales tienen la consideración de especialmente protegidos, y sobre ellos debe plantearse una política de seguridad muy estricta, cuya vulneración implica una infracción muy grave?

SI NO N/A

19.- ¿Se cumple lo establecido en la Ley, en cuanto recoge únicamente los datos pertinentes y no excesivos para la finalidad para la que los recoge, además de no utilizarlos para ningún otro fin?

SI NO N/A

20.- ¿Se encuentran los ficheros de la empresa protegidos contra el acceso no autorizado, tanto física como lógicamente?

SI NO N/A

21.- ¿Están definidos en todo momento qué usuarios tienen acceso a qué ficheros, y cuáles son sus permisos?

SI NO N/A

22.- ¿Se realizan auditorías internas o externas de aplicación de la Ley, al menos cada 2 años?

SI NO N/A

23.- ¿Dispone la compañía de sistemas de destrucción de documentos que evitan que su información se divulgue sin ningún tipo de control y con posibles sanciones?

SI NO N/A

24.- ¿Están expresamente autorizados, o justificados, los envíos electrónicos de material publicitario por los destinatarios?

SI NO N/A

25.- ¿Cumple su empresa con todos los requisitos que obliga la ley de servicios de la sociedad de la información y comercio electrónico (SSI-CE)?

SI NO N/A

26.- ¿Ofrece la empresa al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines publicitarios o promocionales mediante un procedimiento sencillo y gratuito?

SI NO N/A

27.- ¿En su actuación evita al máximo la empresa incurrir en las infracciones detalladas en la ley de los servicios de la sociedad de la información y comercio electrónico (SSI-CE)?

SI NO N/A

28.- ¿Tiene en pleno funcionamiento la empresa un sistema eficaz que evita la pérdida tiempo causada por la recepción de SPAM?

SI NO N/A

29.- ¿Se evita abrir, y ya no digamos responder, a los e-mails sospechosos, que en muchos casos son sugerentes y atractivos?

SI NO N/A

30.- ¿La empresa dispone de medidas de seguridad para combatir con eficacia los delitos del ciberespacio?

SI NO N/A

31.- ¿Se comprueba frecuentemente que la página web en la que se ha entrado es una dirección segura?

SI NO N/A

32.- ¿La empresa ha acomodado su política de protección de datos, a lo prescrito por el RGPD de la UE?

SI NO N/A

33.- ¿Ha efectuado la empresa un estudio sobre su actuación de acuerdo con el RGPD de la UE en el que se han localizado las posibles infracciones y se han calculado las sanciones correspondientes?

SI NO N/A

34.- ¿Existe en la empresa la figura del responsable del fichero y ejerce sus funciones y obligaciones plenamente?

SI NO N/A

35.- ¿Dispone la web de la empresa de la adecuada protección legal?

SI NO N/A

36.- ¿Se han cerciorado los directivos de la empresa que ésta no está sometida a algunos requisitos administrativos, como el de la comunicación al Registro de ventas a distancia?

SI NO N/A

37.- ¿Recoge la publicidad por internet de la empresa todos los requerimientos que exige la actual legislación sobre aquella?

SI NO N/A

38.- ¿Es satisfactorio el uso de las cookies establecidas en la web de la empresa?

SI NO N/A

39.- ¿Se ha asegurado la compañía que todos sus proveedores cumplen con la normativa de la protección de datos?

SI NO N/A

40.- ¿Tiene la empresa redactados el registro de actividades de tratamiento, en sustitución al alta de ficheros en la AEPD, el análisis de riesgo, las medidas de seguridad a adoptar y cómo actuar en caso de producirse una brecha de seguridad?

SI NO N/A

Ya se han identificado los ítems con respuesta NO. Ahora se trata de seleccionar entre ellos, solamente DOS, pero los que se consideren que son los más importantes y decisivos de cara a su repercusión en los resultados tanto actuales como futuros.

*Sólo resta ponerse a trabajar de inmediato en los mismos para erradicarlos o minimizarlos. Para ello le aconsejamos que siga las recomendaciones descritas en el apartado "**CÓMO SE REALIZA LA IMPLANTACIÓN**"*