Principales obligaciones para las empresas derivadas del RD 43/2021, de 26 de enero, en materia de ciberseguridad

La aprobación del RD 43/2021 supone el pleno desarrollo del marco normativo fijado por el RD-ley 12/2018, que traspuso a su vez la Directiva NIS al Ordenamiento jurídico español.

Al mismo tiempo, establece un gran número de nuevas obligaciones para los **Operadores de Servicios Esenciales y Prestadores de Servicios Digitales**.

Las principales obligaciones derivadas del nuevo RD 43/2021 son:

Establecer, según las obligaciones establecidas en el RD, una **Política de seguridad de redes y sistemas** adaptada a la empresa y sus características, que tenga en cuenta: el modelo de gobernanza de la ciberseguridad ya implantado, el sector de actividad y las especificaciones de la empresa.

Identificar el concreto contenido de **obligaciones aplicables** a la empresa en cada caso y revisar las políticas y protocolos ya existentes para asegurar un correcto cumplimiento normativo.

Obligación de preparar y aprobar una Política de Seguridad de las redes y sistemas y, como consecuencia de ello, preparar y aprobar la **Declaración de Aplicabilidad** para ser entregada a la Autoridad competente en el plazo de 6 meses (Julio 2021).

Determinar el marco de referencia Técnico a implementar siendo preferente el **Esquema Nacional de Seguridad**, aunque son posibles otros marcos de referencia.

Coordinar las actuaciones en materia de ciberseguridad y de **protección de datos** en consonancia con la convergencia ente las dos regulaciones que introduce el RD.

Establecer una **política de gestión de riesgos** respecto a terceros proveedores externos, ya que el RD obliga a gestionar esos riesgos.

Adaptar las cláusulas contractuales respecto a los productos y servicios procedentes de **terceros suministradores** acordes con las nuevas obligaciones.

Establecer una **política y un protocolo de notificaciones** de incidentes a la autoridad competente, conforme a los criterios fijados en la Instrucción Nacional de Notificación y Gestión de Ciberincidentes aprobada en el RD, incluyendo aspectos legales y de comunicación.

Establece un **nuevo estatuto jurídico para el CISO** dentro de la organización, que recoja su nueva posición, responsabilidades ante las autoridad y funciones a realizar: técnicas, organizativas y jurídicas.

Nombrar al CISO en el plazo de tres meses (abril 2021) y dotar a esta figura de los medios necesarios para dar un adecuado cumplimiento a la regulación fijada por el RD.

Valorar la procedencia de iniciar un proceso de **certificación en ENS** u otros marcos de referencia como elemento sustitutivo de la acción supervisora con el objeto de acreditar el cumplimiento de las obligaciones de ciberseguridad.

El nuevo RD 43/2021 supone un antes y un después en el marco regulador de la ciberseguridad. Exige llevar a cabo acciones por parte de las empresas incluidas en su ámbito de aplicación con carácter inmediato, dados los **plazos tan breves** que se han establecido para dar cumplimiento a las obligaciones que establece.

Tiene un alto impacto en la gobernanza de la ciberseguridad de las empresas. Supone la necesidad de adaptar y preparar a las empresas al nuevo marco de cumplimiento normativo, ya que en caso contrario se podrían **derivar responsabilidades**.

Esta norma también puede ser una poderosa **herramienta** para impulsar las iniciativas destinadas a alcanzar un adecuado nivel de ciberseguridad dentro de las empresas obligadas.

Se considera de especial importancia el nombramiento del CIS, la política respecto a terceros proveedores, así como cumplimentar la obligación de entregar a las Autoridades competentes la **Declaración de Aplicabilidad**.

Andersen dispone de las capacidades para acompañar a las empresas en el esfuerzo por adaptarse al nuevo contexto regulatorio que exige un cumplimiento normativo en materia de ciberseguridad más intenso. En consonancia con la rápida transformación digital que estamos viviendo, es necesario tener más presentes que nunca los aspectos jurídicos.

Ese expertise legal se potencia con las capacidades tecnológicas aportadas por la alianza con S2 Grupo y CSV, materializándose en un producto de Smart Compliance adaptado a cada empresa para afrontar la gestión de los riesgos tecnológicos y legales de forma eficiente.

Para más información puede contactar con:

Vicente Moret
Of Counsel
Derecho Procesal
vicente.moret@es.Andersen.com