Las empresas de Seguridad Informática entran en la Seguridad Privada por la puerta de atrás.

Tal vez haya podido pasar desapercibido el artículo 6.6. de la Ley de Seguridad Privada que establece que "***A las empresas, sean o no de seguridad privada, que se dediquen a las actividades de seguridad informática***, entendida como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquéllos prestan, ***por su incidencia directa en la seguridad de las entidades públicas y privadas***, se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten".

Era algo de esperar en la medida que la *ciberseguridad* constituye un área declarada como prioritaria o de especial interés en el artículo 10 de la Ley de Seguridad Nacional.

No ha pasado desapercibido en el nuevo reglamento (borrador) de la Ley de Seguridad Privada, que dedica dentro del Título VIII, disposiciones complementarias, el capítulo V a la seguridad informática (artículos 225 a 227), quedando obligadas en algunos casos a la inscripción en el Registro Nacional de Seguridad Privada (artículo 227 del borrador del reglamento) a través del mecanismo de la declaración responsable.

A estos efectos, el artículo 225 considera ***sujetas a la normativa sobre seguridad privada***, las siguientes actividades informáticas:

a) Instalación o integración y mantenimiento de medidas de seguridad informática, físicas o lógicas orientadas a garantizar la integridad, confidencialidad y disponibilidad de los sistemas de información y comunicación o de la información contenida en ellos (artículo 52.1.c. de la LSP).

b) Los servicios de alojamiento virtual y compartido o almacenamiento de datos digitales prestados a terceros.

c) Los procesos destinados al análisis, monitorización, operación o administración de los sistemas de seguridad informática, y en su caso, respuestas a incidentes o eventos de seguridad de la información en el ámbito de las tecnologías de información y de las comunicaciones, prestados a terceros, a través de centros operativos de seguridad o equipos de respuesta a incidentes de seguridad de la información.

d) La fabricación o desarrollo de software de seguridad, siempre que no sea de propósito general.

A las empresas de seguridad informática se les impone las siguientes obligaciones dependiendo de las actividades que desarrollen:

1. A las que desarrollen las actividades identificadas en las letras a), b) y c) del artículo 225 cuando los realicen a favor de:
   - Proveedores de servicios de la sociedad de la información.
   - Operadores estratégicos no declarados críticos por aplicación de la normativa sobre protección de instalaciones críticas.
   - Sujetos obligados por el reglamento a adoptar medidas de seguridad informática.
   - Operadores declarados críticos por la aplicación de la normativa sobre protección de instalaciones críticas.

   Estas empresas de seguridad informática deben:
   - ► Inscribir en el registro de Registro Nacional (o autonómico) de Seguridad Privada mediante una declaración responsable aportando la información contenida en el Título V del Anexo I del reglamento.
   - ► Disponer de la certificación ISO 9001.
   - ► Disponer de la certificación ISO 27001.
   - ► Disponer de la certificación ISO 20000.

2. A las empresas que desarrollen que presten los servicios señalados en las letras a), b) o c) del artículo 225 fuera del alcance señalado y las que desarrollen el resto de actividades de seguridad informática contenidas en el artículo 225.
   Estas empresas no deben inscribirse en el Registro Nacional de Seguridad Privada, pero deben:
   - ► Someterse a auditorías externas (artículo 238 del borrador del reglamento).

De la lectura del artículo 226 del borrador del reglamento podría entenderse que no es así y que se refiere sólo a las empresas de seguridad informática identificadas en el punto 1 en la medida que el punto 2 señala que "igualmente, deberán someterse a ***auditorías externas***" y podría pensarse que se refiere sólo a las obligadas a la inscripción en el Registro.

Sin embargo, creo que la interpretación correcta es la señalada y que deben someterse a las auditorías señaladas en los artículos 238 y 239 en la medida que si no son sometidas a algún tipo de requisito del reglamento de seguridad privada no se entiende su consideración en el citado reglamento; por otra parte, las certificaciones citadas (ISO 9001, ISO 27001 e ISO 20000) implican la realización de auditorías anuales, por lo que resulta innecesario obligarles a realizar las auditorías que por la normativa de certificación ya están obligadas a realizar; y por último el artículo 226 lleva por título "requisitos de las empresas prestadoras" refiriéndose a todas las que desarrollan las actividades señaladas en el artículo 225.

MIGUEL ANGEL VILA ESPESO · 963 943 905 · miguelangel@vila-abogados.es · www.vila-abogados.es