El responsable de Seguridad de la Información y la necesidad de armonizar la normativa

César Álvarez Fernández / Coordinador de Proyectos de la Fundación Borredá

El Real Decreto Ley 12/2018, de seguridad de las redes y sistemas de información, que transpone la Directiva 2016/1148 del Parlamento Europeo y del Consejo, más conocida como Directiva NIS, establece la obligación para los operadores de servicios esenciales de designar un responsable de la Seguridad de la Información (RSI). Esta figura, que puede ser una persona, unidad u órgano colegiado, debe actuar como punto de contacto y de coordinación técnica con la autoridad competente.

Su creación es un indudable acierto del legislador español, dado que no aparece en la Directiva que se transpone. En este sentido, hay que recordar que la Directiva 2008/114, sobre protección de infraestructuras críticas (PIC), establecía para los operadores críticos la obligación de designar un responsable de Enlace para la seguridad, que asumiría la función de punto de contacto para cuestiones de seguridad entre el propietario u operador de la infraestructura y la autoridad competente del Estado miembro. Esta diferencia de tratamiento suscita alguna reflexión, especialmente en el momento en que se está configurando un modelo que, tratándose de seguridad, debe ser armónico y eficiente.

Modelo PIC

Hay que hacer notar que la Directiva PIC no habla de un responsable de Seguridad, sino de un **responsable de Enlace para la seguridad**. En cualquier caso, el legislador español, al transponer la Directiva (Ley 8/2011), avanza en el concepto y exige al operador la designación de un **responsable de Seguridad y Enlace** (RSE), además de un delegado de Seguridad por cada una de sus infraestructuras consideradas críticas. En todo caso, la Ley impone que el RSE designado deberá contar con la habilitación de director de Seguridad expedida por el Ministerio del Interior, según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, en función de su normativa específica. Se trata, evidentemente, de un requisito mínimo para garantizar la cualificación técnica del designado, en su doble función de responsable de Seguridad y de Enlace con la Administración.

El Real Decreto 704/2011, que desarrolla la Ley PIC, no especifica las funciones del RSE en tanto que responsable de seguridad, sino únicamente en su faceta de enlace: "el responsable de Seguridad y Enlace representará al operador crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento, canalizando, en su caso, las necesidades operativas e informativas que surjan al respecto". No obstante, en cuanto a su faceta de responsable de Seguridad, la normativa de seguridad privada es clara, no solo en la atribución de funciones y responsabilidades al director de Seguridad, sino al exigir la cualificación necesaria para obtener la habilitación como tal.

Desconocemos si la intención del legislador era regular las funciones de los responsables de Seguridad de los operadores críticos o solo garantizar con su presencia un enlace técnicamente capacitado. Lo cierto es que, bajo esta normativa, los operadores críticos vienen designando como RSE tanto a su responsable de Seguridad como a otros miembros de sus respectivos departamentos de Seguridad que cuenten con la habilitación correspondiente. En cualquier caso, queda ahí un espacio de mejora para que en futuras revisiones se defina mejor la posición de esa importante figura.

Pero la normativa sobre protección de infraestructuras críticas va aún más allá, y establece los mecanismos de comunicación para ámbitos específicos, como la seguridad de la información. Así, el Plan Nacional de Protección de las Infraestructuras Críticas, actualizado por la Instrucción de la Secretaría de Estado de Seguridad número 1/2016, establece que, en el ámbito de la ciberseguridad, los puntos naturales de interlocución serán el jefe de Seguridad de la Información Corporativo (CISO) y/o los equipos de Seguridad de las Tecnologías de la Información de las respectivas organizaciones, por un lado, y el CERTSI (hoy, Incibe-CERT), por otro; sin perjuicio de que **esta relación se efectuará a través de la Oficina de Coordinación Cibernética del CNPIC** (Centro Nacional de Protección de Infraestructuras y Ciberseguridad) **y con el conocimiento del respectivo RSE**.

Es decir, admitiendo la conveniencia de contemplar vías de interlocución específicas para determinados temas, se subordinan al canal establecido para la interlocución genérica, definido por el RSE y el CNPIC (OCC, Oficina de Coordinación Cibernética). No podría ser de otra forma habida cuenta de la necesidad de unificar responsabilidades en materia de seguridad, función crítica para las organizaciones, que no admite descoordinación en sus acciones de ejecución.

Modelo de seguridad privada

En este ámbito, nuestra legislación viene centrándose tradicionalmente en la regulación de las empresas de seguridad privada como proveedores de servicios de seguridad. No obstante, la Ley 5/2014, mirando también al usuario de estos servicios, ofrece, por primera vez, una regulación completa de la figura del director de Seguridad, al que coloca en el centro del modelo y le asigna una batería de funciones de extraordinaria trascendencia para la organización de los servicios privados en las compañías y entidades que los utilicen. Sin entrar en el análisis exhaustivo de las funciones recogidas en el artículo 36, quiero hacer especial mención a dos de ellas, verdaderamente significativas. Primeramente, al **artículo 36.1.c)**, que encomienda al director de Seguridad "la planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a **prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza** con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables". Y, por otra parte, al **artículo 36.1.h)**, que le atribuye "la **interlocución y enlace con la Administración**, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o grupo empresarial que les tenga contratados, **en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos**".

Parece evidente la intención del legislador de unificar en el director de Seguridad las numerosas figuras, creadas por diferentes normas, para servir de enlace con diferentes órganos de la administración en otras tantas materias.

Para llevar a cabo tan importantes funciones, el legislador de 2014 diseña un **elevado perfil profesional** para el director de Seguridad, al que exige "la obtención bien de un **título universitario oficial de grado en el ámbito de la seguridad** que acredite la adquisición de las competencias que se determinen, o bien del título del curso de dirección de seguridad, reconocido por el Ministerio del Interior" (artículo 29.1.b).

A falta del reglamento de desarrollo, resulta obvio que esta segunda vía de acceso a la profesión no podrá ser otra que un curso de postgrado en materia de seguridad, con el que graduados en cualquier materia adquieran las competencias específicamente necesarias para la dirección de seguridad de empresas y entidades.

Por otro lado, un aspecto capital de la Ley de Seguridad Privada es la exigencia de que **los directores de Seguridad de las entidades obligadas a disponer de ellos desempeñen sus funciones integrados en las plantillas de dichas empresas**. El legislador trata así de establecer con claridad que la persona que está llamada a ser el centro de la planificación, organización y control de los servicios y medidas de seguridad debe formar parte de la empresa que los utiliza, para garantizar su fidelidad y alineación con los objetivos de esta frente a hipotéticas contradicciones con los intereses de un proveedor externo.

Por lo que se refiere a la seguridad de la información, la Ley 5/2014 contem-

pla, por primera vez, la posibilidad de imponer requisitos específicos a las empresas, sean o no de seguridad privada, que se dediquen a las actividades de **seguridad informática**, por su incidencia directa en la seguridad de las entidades públicas y privadas y para garantizar la calidad de los servicios que presten. Es decir, se centra en los proveedores de servicios de seguridad informática, tratando de proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquellos prestan.

Evidentemente, en el concepto de seguridad informática utilizado en la Ley se debe incluir la **seguridad de la información**, del dato como uno de los principales activos de las empresas, entendida como una subespecie de la seguridad digital que se ocupa de cualquier evento producido en dicho entorno.

Desgraciadamente, la Ley de Seguridad Privada, que debería regular las aportaciones del sector privado a la seguridad pública, peca de falta de ambición por no entrar de lleno a considerar la mayor amenaza que se cierne hoy sobre nuestras empresas y entidades. Esto es, por no atender prioritariamente a la seguridad de la información como uno de los principales activos a proteger, considerando, tal vez, que otras normas habrían de asumir ese papel. Dicho esto, quizá tuviera razón el legislador en 2014, y haya sido preferible esperar a la normativa europea en un tema donde las interconexiones e interdependencias aconsejan adoptar soluciones comunes en todos los Estados miembros de la Unión.

No obstante, **queda meridianamente establecido en esta ley el principio de unificar en la figura del director de Seguridad la responsabilidad de la gestión de la seguridad frente a todo tipo de riesgos**.

Modelo NIS

La Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida también como Directiva NIS, crea las figuras del operador de servicios esenciales y del proveedor de servicios digitales y les impone una serie de obligaciones en materia de seguridad y de notificación de incidentes. Esta Directiva, no crea, en cambio, ninguna obligación de que estos nuevos actores dispongan de ningún tipo de responsable en materia de seguridad o de enlace con las autoridades competentes. No porque no sea necesario, sino debido a que, en este caso, deja a los Estados miembros libertad para regular el cumplimiento de las obligaciones impuestas.

La Ley de Seguridad Privada peca de falta de ambición por no atender prioritariamente a la seguridad de la información como uno de los principales activos a proteger

Al transponer la Directiva a nuestro ordenamiento, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, establece que "los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano colegiado **responsable de la Seguridad de la Información**, como punto de contacto y de coordinación técnica con aquella". El Real Decreto-ley se limita a implantar la figura del RSI, ya existente en el ámbito del Esquema Nacional de Seguridad, sin entrar en otras consideraciones, ni siquiera en la determinación de sus funciones específicas, que deja al desarrollo reglamentario.

En cuanto a este reglamento, en fase de elaboración, recientemente hemos tenido acceso al Proyecto de Real Decreto que lo contiene, sometido al trámite de audiencia y de información pública por la Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa. Este proyecto, que efectivamente se ocupa en profundidad de la figura y las funciones del RSI, contiene algunas previsiones que generan importantes dudas sobre su grado de madurez en lo que le respecta.

En efecto, tras imponer a los operadores de servicios esenciales la obligación de aprobar una política de seguridad de las redes y sistemas de información, dispone la elaboración de un documento denominado *Declaración de aplicabilidad de medidas de seguridad* en el que se relacionen las efectivamente adoptadas, que **deberá ser suscrito por el responsable de seguridad del sistema de información del operador**. Pero no deja de generar cierta confusión esta denominación, máxime cuando entre los requisitos a cumplir por el RSI figura textualmente el de "mantener la debida independencia respecto de los responsables de Sistemas de Información". Por cierto, siendo loable y muy acertada esta última previsión, el legislador podría contribuir a la claridad de su exposición con alguna otra expresión más adecuada, del tipo "en el ejercicio de sus funciones actuará con independencia funcional respecto a los responsables de Sistemas de la Información".

En cuanto a estos requisitos, hay alguna otra previsión de difícil encaje en el sistema que ha venido construyéndose para los responsables de Seguridad. Tal es el caso del que impone "ostentar una posición en la organización que facilite el desarrollo de sus funciones, en particular la comunicación real y efectiva con la alta dirección". Resulta insólito que el legislador quiera interferir en la estructura de la organiza-

ción, porque su acción debería limitarse a crear un marco de responsabilidades que implique a la alta dirección, sin pretender ubicar al RSI en una determinada posición en el organigrama de la empresa. También hay que calificar como un vano ejercicio de voluntarismo el requisito de "contar con los recursos necesarios para el desarrollo de dichas funciones". Siendo lógica esta pretensión, ¿quién es el sujeto de la obligación?, ¿el RSI, la alta dirección? ¿Quién evalúa la adecuación de los recursos a las necesidades?

Respecto a las funciones atribuidas al RSI, la de "actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos", puede conducir a la invasión de las competencias de los responsables de otras áreas. En sentido positivo, hay que reconocer el acierto de establecer la compatibilidad entre las funciones de RSI y las de RSE, responsable de Seguridad del Esquema Nacional de Seguridad y delegado de Protección de Datos, aunque en este último caso la compatibilidad no resulte tan pacífica a la vista de algunos informes de la Agencia de Protección de Datos. Lo que no resulta tan plausible es que el propio reglamento habilite un cajón de sastre para asignar al RSI "cualesquiera otras funciones que se determinen reglamentariamente".

Pero, definitivamente, el gran fallo de esta nueva regulación radica en que **no fija ningún requisito de formación para el RSI**, que, obviamente, debe estar bien cualificado para desarrollar las funciones encomendadas. Le exige, en cambio, "contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico", sin establecer tampoco ningún estándar de referencia. Por otra parte, nada dice el proyecto de reglamento respecto a la relación del RSI con su empresa, hasta el punto de que, con la redacción actual, podría ser un empleado del proveedor externo de los servicios en los, muy previsoramente, le autoriza a apoyarse.

Conclusiones

Como principales conclusiones de todo lo expuesto destaco las siguientes:

- El bloque normativo de seguridad está mayoritariamente auspiciado por el Ministerio del Interior, que ha unificado la responsabilidad de la gestión de todo tipo de riesgos de empresas y entidades en torno a la figura del director de Seguridad, integrado en la estructura del usuario en los supuestos más críticos.
- Las funciones que le atribuye la Ley de Seguridad Privada proyectan al director de Seguridad hacia una posición preeminente, con responsabilidad global sobre la seguridad de su organización, que está en condiciones de asumir dada su formación específica.
- La normativa PIC no desarrolla las funciones del RSE más que como responsable de enlace con las autoridades competentes, pero afianza claramente su autoridad en esta materia frente a otros enlaces técnicos que puedan establecerse.
- Con la intervención del Ministerio de Economía y Empresa al transponer la Directiva NIS y pretender regular una figura de nuevo cuño, como el RSI, se desvirtúa el modelo establecido por el Ministerio del Interior, pues aparece un nuevo actor que viene a ejercer sus funciones al margen de los canales predeterminados.
- Nada impide que las empresas y entidades integren en sus departamentos de Seguridad especialistas en áreas concretas de riesgos, siempre que su actuación se produzca bajo la dirección y responsabilidad del correspondiente director de Seguridad Corporativo.
- Es imprescindible regular la formación del RSI en base a estándares conocidos u otros diseñados expresamente a este efecto. Igualmente, debe establecerse claramente la necesidad de que forme parte de la estructura del operador de servicios esenciales.
- El proyecto de Real Decreto que desarrolla el Real Decreto-ley NIS es parte del bloque normativo de seguridad y debería armonizar sus disposiciones con otras que también lo integran. Según la acertada definición del Esquema Nacional de Seguridad, la seguridad debe entenderse como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. Este principio excluye cualquier actuación puntual o tratamiento coyuntural. S