

ASIET

PREGUNTA CONSULTA SUBTEL	COMENTARIO RECIBIDO
<p>Artículo 7.</p>	<p>Debemos señalar que la obligación de notificar ciberincidencias por parte de los operadores plantea unos tiempos para la emisión del reporte una vez detectada dicha incidencia muy estrictos (Desde 30 minutos para incidentes de carácter grave a 3 horas para incidentes de bajo impacto)</p> <p>A nuestro entender estos tiempos debieran ser más flexibles o bien determinar con mayor claridad qué debe ser incluido en la primera notificación.</p> <p>Si observamos la legislación europea en la materia (a través de la Directiva de Seguridad de las Redes y de la Información NIS) y más en concreto la española (Guía Nacional de Notificación y Gestión de Ciberincidentes), se plantea que el incidente debe ser notificado una vez se tenga conocimiento del mismo, sin embargo se establece una suerte de comunicación intermedia (De 24 a 48 h para los casos más graves y 72 para el resto una vez se produjo la notificación inicial) que consiste en un informe mediante el cual se aportan los datos disponibles en ese momento relativos al incidente comunicado. Esto da un mayor margen a los operadores, permitiendo que el reporte que finalmente se envíe, sea más certero y se pueda centrar la actuación inicial del operador en solucionar la ciberincidencia.</p>

	<p>Sería conveniente que en la normativa se pudiera tener en cuenta ejemplos como el europeo, de modo que se adopten criterios más flexibles para la notificación y emisión del reporte. Si no se hiciera así, nos podríamos encontrar con diferentes niveles de madurez en cada una de las empresas para la gestión de la crisis, por lo que a algunas no tendría capacidad de poder identificar el nivel de criticidad del incidente en tan poco tiempo. De la misma forma podría resultar interesante la posibilidad de establecer un glide path para que los tiempos de reporte pudieran ir disminuyéndose de forma paulatina, conforme se disponga de más evidencia recolectada en la aplicación de la normativa.</p>
--	--