Resumen Real Decreto Ley 12/2018

Transposición Directiva Europea NIS

Comisión Ciberseguridad

Ametic

https://ametic.es/es

Contenido

Ámbito de aplicación

La ley aplica a:

Empresas establecidas en España* que operen en el ámbito de:

a) Los **operadores de servicios esenciales** (en adelante "**OSE**") dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos: Administración, Espacio, Industria Nuclear, Industria Química, Instalaciones de investigación, Agua, Energía, Salud, TIC y Transporte.

b) Empresas grandes o medianas que sean **proveedores de servicios digitales** (en adelante "**PSD**") en el ámbito de:

- **mercados en línea**
- **motor de búsqueda en línea**
- **servicios de computación en nube**

**Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión*

Ametic

Ámbito de aplicación

La ley NO aplica a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza **que no sean designados como operadores críticos.**

b) Los proveedores de servicios digitales cuando se trate de **microempresas o pequeñas empresas**

Autoridad competente

Para los PSD la autoridad competente en materia de seguridad de las redes y sistemas de información es **la Secretaría de Estado para el Avance Digital, del Ministerio de Economía y Empresa.**

El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

Comunicación de actividad

Los PSD señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

Los PSD que ya vinieran prestando servicios deberán comunicar su actividad en el plazo de tres meses desde la entrada en vigor de este Real Decreto-Ley*.

La comunicación se realizará a través de la sede electrónica del Gobierno en:

https://sede.minetur.gob.es/es-es/procedimientoselectronicos/Paginas/detalle-procedimientos.aspx?IdProcedimiento=209

**Los plazos han sido modificados posteriormente a la publicación del RDL.*

Funciones de las autoridades competentes

Supervisión de las obligaciones y ejercer la potestad sancionadora

Informar al público sobre determinados incidentes, cuando sea necesario

Promover el uso de normas y especificaciones técnicas

Establecer canales de comunicación con:

- **los OSE**
- **los PSD**
- **los CSIRT de referencia**
- ***El Punto de contacto único*** **(Consejo de Seguridad Nacional a través del Departamento de Seguridad Nacional)**

Recibir notificaciones sobre incidentes que sean presentadas a través de los CSIRT e informar de ellas al punto de contacto único

Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes.

Cooperar con las autoridades competentes de otros Estados miembros de la UE

Cooperar con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, ciudadana y seguridad nacional.

Ametic

Equipos de respuesta a incidentes de seguridad informática de referencia (CSIRT)

El CSIRT de referencia para los PSD será el INCIBE-CERT salvo que estén comprendidos en la comunidad de referencia del CCN-CERT (públicos)

Sus funciones son:

- Supervisar incidentes a escala nacional
- Difundir alertas, avisos e información sobre riesgos e incidentes entre los interesados
- Responder a incidentes
- Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación
- Participar en la red de CSIRT

Obligaciones de seguridad

Los PSD deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para:

- Gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios.
- Prevenir y reducir al mínimo el impacto de los incidentes que les afecten.

Aspectos y avances técnicos que deben tener en cuenta los PSD a la hora de aplicar sus medidas de seguridad:

- La seguridad de los sistemas e instalaciones
- La gestión de incidentes
- La gestión de la continuidad de las actividades
- La supervisión, auditorías y pruebas
- El cumplimiento de las normas internacionales

Obligaciones de notificación

Los PSD notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios.

Teniendo en cuenta que:

La obligación de la notificación del incidente únicamente se aplicará cuando el PSD tenga acceso a la información necesaria para valorar el impacto de un incidente.

Las notificaciones del PSD se referirán a los incidentes que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados, tanto si se trata de redes y servicios propios como si lo son de proveedores externos.

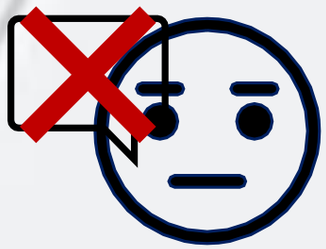
Las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

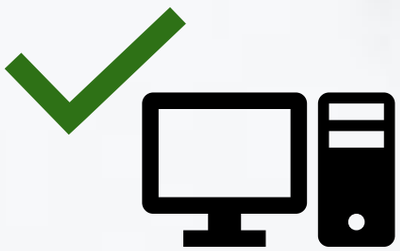
Notificación de Incidentes

La importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

- El número de usuarios afectados por la perturbación del servicio esencial
- La duración del incidente
- La extensión o áreas geográficas afectadas por el incidente
- El grado de perturbación del funcionamiento del servicio
- El alcance del impacto en actividades económicas y sociales cruciales.
- La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial
- El daño a la reputación

Los PSD podrán omitir información de la que aún no dispongan relativa a su repercusión sobre servicios. Tan pronto como la conozcan deberán remitirla a la autoridad competente o informar, tras un tiempo prudencial, de las actuaciones realizadas para reunir la información y de los motivos por los que no ha sido posible obtenerla.





Un incidente se considerará resuelto cuando se hayan restablecido las redes y sistemas de información afectados y el servicio opere con normalidad

Ametic

Notificación de incidentes

La autoridad competente podrá exigir a los PSD que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en beneficio del interés público.

También podrá decidir informar de modo directo al público o a terceros sobre el incidente. En estos casos la autoridad competente consultará y se coordinará con el PSD antes de hacerlo.

Los PSD tienen la obligación de resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes, aportando la información requerida por este para analizar la naturaleza, causas y efectos de los incidentes notificados

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad

Ametic

Supervisión

La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones cuando tenga noticia de:

Algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia, pudiendo requerir al PSD que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

Incidentes que perturben de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medidas de supervisión pertinentes.

Ametic

Régimen Sancionador

Las infracciones se clasifican en:

Muy Graves

- No adoptar medidas para subsanar deficiencias detectadas cuando estas le hayan hecho vulnerable a un incidente con efectos perturbadores significativos en el servicio y previamente al incidente no hubiera atendido los requerimientos dictados por la autoridad competente.
- Incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio. Se considerará reiterado a partir del segundo incumplimiento.
- No tomar las medidas necesarias para resolver los incidentes cuando estos tengan un efecto perturbador significativo en la prestación de servicios digitales en España o en otros Estados miembros.

Graves

- No adoptar las medidas para subsanar las deficiencias detectadas en respuesta a un requerimiento cuando sea el tercer requerimiento desatendido en los 5 últimos años.
- No notificar incidentes con efectos perturbadores significativos en el servicio.
- Demostrar falta de interés en la resolución de incidentes con efectos perturbadores significativos notificados cuando dé lugar a una mayor degradación del servicio.
- Proporcionar información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad.
- Poner obstáculos a la realización de auditorías.

Leves

- Incumplimientos que no sean graves o muy graves.
- No adoptar las medidas para corregir las deficiencias detectadas ante un requerimiento de subsanación.
- No facilitar la información completa o de forma tardía a las autoridades competentes o al CSIRT.
- La ausencia o falta de información en la notificación de los sucesos o incidencias.
- No remitir el informe justificativo sobre la imposibilidad de reunir la información.
- No seguir las indicaciones que reciba del CSIRT de referencia para resolver un incidente.

Ametic

Régimen Sancionador

Se impondrán las siguientes multas o sanciones a los infractores:

Muy Graves

500.001€ hasta 1.000.000€

Graves

100.001€ hasta 500.000€

Leves

amonestación o multa hasta 100.000€

Las sanciones firmes en vía administrativa por infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el «Boletín Oficial del Estado» y en el sitio de Internet de la autoridad competente.

Ametic

Régimen Sancionador

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

- El grado de culpabilidad o la existencia de intencionalidad.
- La continuidad o persistencia en la conducta infractora.
- La naturaleza y cuantía de los perjuicios causados.
- El número de usuarios afectados.
- La reincidencia en el último año de más de una infracción de la misma naturaleza.
- El volumen de facturación del responsable.
- La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.
- Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.

Pueden ser atenuantes de la sanción o motivo únicamente de sanción las siguientes medidas:

- Regularizar la situación irregular de forma diligente.
- Reconocer espontáneamente su culpabilidad.
- No hubiese sancionado o apercibido al infractor en los dos años previos.

Ametic