ASEPEC

IMPACTO DEL NUEVO REGLAMENTO DE EJECUCIÓN DE NIS2 EN LOS PRESTADORES DE SERVICIOS DE CONFIANZA CUALIFICADOS (QTSP)

Se ha publicado recientemente el Reglamento de Ejecución de la Directiva NIS2, que establece requisitos técnicos y metodológicos vinculados a la gestión de incidentes[1]. Este Reglamento tiene un impacto directo en los Prestadores de Servicios de Confianza Cualificados (QTSP), expresamente en relación con su artículo 14, que introduce exigencias adicionales para la gestión de incidentes, imponiendo a los QTSP nuevas obligaciones con enfoque en la prevención, detección, respuesta y mitigación de riesgos.

A continuación, se detallan los **principales requisitos técnicos y metodológicos** que los QTSP deberán implementar para cumplir con la normativa:

1. Gestión Proactiva de Incidentes

Los QTSP deben adoptar un enfoque preventivo en la gestión de incidentes, identificando, evaluando y mitigando vulnerabilidades en su infraestructura antes de que se conviertan en amenazas reales. Esto incluye la implementación de sistemas de monitorización continua que permitan detectar eventos anómalos y señales de alerta en tiempo real.

2. Notificación de Incidentes Significativos

El Reglamento impone una obligación de notificación inmediata de incidentes significativos a las autoridades competentes. Los QTSP deberán reportar cualquier evento que pueda comprometer la seguridad, la disponibilidad o la integridad de los servicios cualificados que prestan, detallando el impacto del incidente, las medidas tomadas y los planes de mitigación. La notificación deberá realizarse en un plazo determinado para garantizar la pronta intervención y coordinación con las autoridades.

3. Capacidades de Respuesta y Recuperación

Es fundamental que los QTSP cuenten con un plan de respuesta ante incidentes detallado y robusto, que permita actuar de manera rápida y efectiva para contener cualquier amenaza o brecha de seguridad. Este plan debe incluir protocolos para la recuperación de servicios, minimizando el tiempo de inactividad y el impacto en los usuarios finales, así como mecanismos de análisis post-incidente para identificar las causas que lo provocaron y mejorar los procesos futuros.

4. Evaluación y Mitigación de Riesgos

El Reglamento exige que los QTSP realicen una evaluación continua de riesgos en relación con sus servicios y las infraestructuras que los soportan. Esta evaluación debe incluir amenazas tanto internas como externas, como ciberataques, fallos técnicos o errores humanos. A partir de esta evaluación, los QTSP deberán implementar medidas de mitigación adecuadas, tales como controles de acceso mejorados, cifrado de comunicaciones y respaldo de datos en ubicaciones seguras.

[1] https://digital-strategy.ec.europa.eu/en/library/nis²-commission-implementing-regulation

5. Colaboración y Coordinación

El Reglamento refuerza la importancia de la coordinación entre QTSP y las autoridades nacionales competentes. Se espera que los prestadores de servicios trabajen en estrecha colaboración con los Organismos de Supervisión para intercambiar información sobre amenazas emergentes y vulnerabilidades. Además, los QTSP deberán participar en ejercicios conjuntos de simulación de incidentes y mejorar la interoperabilidad con los sistemas nacionales de gestión de incidentes, como el CSIRT en España.

Con enfoque en la seguridad de la información y de las redes, debiendo establecerse a intervalos planificados y cuando se produzcan incidentes importantes o cambios significativos en las operaciones o los riesgos.

6. Relevancia de la Cadena de Suministro

El Reglamento destaca la importancia de evaluar y tener en cuenta la calidad general y resiliencia de los productos y servicios que conforman la cadena de valor de los QTSP, y las medidas de gestión de riesgos de ciberseguridad en sus procesos y en los acuerdos contractuales con los proveedores directos y con los prestadores de servicios con el objeto de disminuir los riesgos detectados para la seguridad de las redes y los sistemas de información.

Asimismo, entre otros aspectos, los QTSP deberán revisar de forma periódica los acuerdos de nivel de servicio y analizar los riesgos que puedan presentar los cambios en productos o servicios TIC de sus proveedores y prestadores de servicios adoptando, en su caso, medidas para su mitigación.

7. Documentación y Auditoría

Los QTSP están obligados a mantener una documentación exhaustiva de todas las actividades relacionadas con la gestión de incidentes. Esto incluye registros detallados de los incidentes, las medidas adoptadas y las revisiones posteriores. Los Certification Assessment Bodies (CAB) revisarán esta documentación durante sus auditorías para verificar la conformidad con los nuevos requisitos de NIS2, así como la eficacia de las medidas implementadas.

7. Protección de Datos y Privacidad

El Reglamento también exige que los QTSP garanticen la protección de los datos personales y otros datos sensibles en todo el proceso de gestión de incidentes. Las medidas de seguridad implementadas deben cumplir con el Reglamento General de Protección de Datos (RGPD), especialmente en lo que respecta a la notificación de violaciones de seguridad que puedan comprometer la privacidad de los usuarios.

Auditorías de los CAB y Supervisión por parte del Ministerio de Asuntos Económicos y Transformación Digital

Con la entrada en vigor del Reglamento de Ejecución de la Directiva NIS2, se ha producido un cambio significativo en el marco normativo aplicable a los Prestadores de Servicios de Confianza Cualificados. Una de las modificaciones más notables es el impacto directo que este Reglamento tendrá en las auditorías realizados por los Certification Assessment Bodies (CAB) y los procesos de supervisión por parte del Ministerio.

Hasta la publicación del Reglamento de Ejecución, la norma ETSI EN 319 401 en su versión 3.1.1., publicada en junio de 2024 y que identifica los controles de la Directiva NIS2 aplicables a los QTSP, estaba programada para ser de aplicación obligatoria para los QTSP a partir del 28 de febrero de 2025. Sin embargo, con la promulgación del Reglamento de Ejecución de NIS2, este calendario ha quedado alterado, dado que el reglamento introduce nuevas exigencias técnicas y metodológicas que se deberán cumplir de manera inmediata tras la entrada en vigor del texto normativo, prevista para 20 días después de su publicación.

Esto significa que las auditorías de cualificación y seguimiento que realicen los CAB incorporarán desde ahora los controles y medidas establecidos en NIS2 y su Reglamento de Ejecución, lo que deja sin efecto el periodo transitorio originalmente estipulado para la adopción plena de la norma ETSI. En otras palabras, aunque algunos QTSP habían planificado realizar adaptaciones a sus sistemas y procesos hasta el 2025, ahora deberán ajustar sus operaciones de manera más acelerada. Los CAB, por su parte, están obligados a adecuar sus prácticas de auditoría para reflejar los requisitos introducidos por el nuevo Reglamento.

Recomendamos a todos los QTSP revisar detenidamente el contenido del nuevo Reglamento y ajustar sus procedimientos internos de gestión de incidentes y seguridad para garantizar el cumplimiento con la normativa vigente, en coordinación con su entidad de auditoría de certificación (CAB), con el Órgano de Supervisión y con otras partes interesadas.

ASEPEC

C/Serrano 69, Madrid. ECIJA HQ
info@asepec.es