ECIJA

Nuevas Exigencias de Ciberseguridad NIS2 para los Prestadores de Servicios Electrónicos de Confianza

NOTA INFORMATIVA

30.09.2024

Nuevas Exigencias de Ciberseguridad NIS2 para los Prestadores de Servicios Electrónicos de Confianza

SEPTIEMBRE 2024

La norma técnica aplicable a todos los Prestadores de Servicios Electrónicos de Confianza (ETSI 319 401) se modifica para incorporar las obligaciones y controles de ciberseguridad de NIS2

La prestación de servicios electrónicos de confianza se considera un elemento esencial de la infraestructura digital europea. Así se cita expresamente en la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un nivel elevado común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva 2016/1148 (**Directiva NIS2 o NIS2**).

NIS2 identifica en su artículo 3 que los requisitos para las medidas de gestión de riesgos de ciberseguridad son aplicables, como entidades esenciales, a los **Proveedores Cualificados de Servicios de Confianza** (en adelante TSP) según el Reglamento eIDAS.

Con fecha 30 de mayo se ha adoptado la norma técnica que especifica los requisitos normativos sobre el funcionamiento y las prácticas de gestión de los Prestadores de servicios electrónicos de confianza, independientemente del servicio que presten (ETSI 319 401) adaptada a los requisitos de NIS2. Esta adaptación ha conseguido que se apliquen las mismas obligaciones y controles derivados de NIS2 a todos los prestadores de servicios electrónicos de confianza cualificados de la Unión Europea, acercándose a la idea del mercado único y que los Prestadores puedan prestar sus servicios en cualquier país sin limitaciones.

Además, partiendo de la base que dicha norma técnica ya había incorporado todos los requisitos exigibles a un sistema de gestión de la seguridad de la información, con el hecho de que ahora incorpore los requisitos exigibles en materia de Ciberseguridad identificados en la norma NIS2, contribuye a la prestación de los servicios con una alta calidad y confiabilidad, incorporando medidas de seguridad más robustas y efectivas que reducen riesgo y fortalecen el crecimiento y desarrollo del sector, beneficiando a la economía en general.

[1]Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE

Ahondando más en las incorporaciones de los requisitos exigidos a los TSP por NIS2, conviene destacar que muchos de ellos ya estaban incluidos en la ETSI (en su versión anterior); no obstante, a continuación**, se destacan las novedades**:

- **El personal directivo deberá poseer experiencia o formación** en relación con el servicio de confianza que se preste, familiaridad con los procedimientos de seguridad para el personal con responsabilidades de seguridad y experiencia en seguridad de la información y en evaluación de riesgos de ciberseguridad suficientes, para desempeñar las funciones de dirección. Asimismo, deberá proporcionar liderazgo y apoyo en la formación y capacitación en ciberseguridad y fomentar una cultura de ciberseguridad en toda la organización, promoviendo la conciencia y la responsabilidad de todos los empleados y proveedores de la cadena de suministro respecto a la protección de la información y los sistemas.

- El TSP deberá establecer **un procedimiento específico para notificar los cambios importantes en la prestación del servicio de confianza** a las partes correspondientes.

- El TSP deberá **identificar al menos a una persona responsable de la seguridad de la red y de la información** que informe a la alta dirección. En aquellos TSP certificados conforme a ISO 27001 este rol podría ser asumido por el Responsable del SGSI u otra persona que designe la dirección de la organización.

- El TSP deberá mantener un inventario de activos detallado y preciso para garantizar una gestión eficaz de vulnerabilidades técnicas y deberá asignar un nivel de clasificación a cada activo, o grupo de activos, en función de los requisitos de protección de la confidencialidad, integridad, autenticidad y disponibilidad, y de acuerdo con su evaluación de riesgos y valor empresarial.

- Para reforzar la seguridad de los recursos humanos y la gestión de activos se introduce como novedad el deber del TSP de **identificar, documentar e implantar normas para el uso aceptable de la información y otros activos asociados,** así como incluir en los procedimientos de gestión de altas y bajas de recursos humanos, regulaciones sobre la devolución de todos los activos físicos y electrónicos propiedad del TSP que le hayan sido confiados. Esta medida debe preverse para el personal interno y externo, contratistas u otros terceros.

- El TSP utilizará **procedimientos sólidos de autorización para las cuentas con privilegios.** Las cuentas con privilegios sólo se utilizarán si los privilegios son necesarios para la actividad específica como la que desempeñan los roles de confianza. Los permisos de acceso a cuentas privilegiadas deberán ser monitorizados por el TSP a intervalos planificados y modificarse en función de los cambios organizativos. Se documentará el resultado de la revisión, incluidos los cambios necesarios de los derechos de acceso.

El TSP deberá adoptar, o mejorar la cobertura y el funcionamiento de las medidas de autenticación para usuarios y dispositivos, incluido, cuando proceda, el uso de mecanismos de autenticación multifactor o una solución de autenticación continua, como voz, vídeo y texto seguros, antes de acceder a la red del TSP y a los sistemas de información ITS, en función de la clasificación de los sistemas a los que se vaya a acceder.

- Cuando el **personal trabaje a distancia**, el TSP deberá implementar medidas de ciberseguridad para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones del TSP.

Los TSP que permitan actividades de trabajo a distancia deberán publicar **una política específica sobre el trabajo a distancia** que defina las condiciones y restricciones de ciberseguridad pertinentes.

- El TSP deberá **establecer, documentar, implementar, supervisar y revisar las configuraciones**, incluidas las de seguridad, del hardware, el software, los servicios y las redes. En este sentido, el TSP deberá desplegar herramientas de gestión y supervisión automatizada de los sistemas.

- El TSP deberá mantener **copias de seguridad de la información** y recursos suficientes, incluidas las instalaciones, la red y los sistemas de información, así como el personal, de acuerdo con la evaluación de riesgos y el plan de continuidad de las actividades.

- El TSP deberá tomar medidas para reforzar la seguridad de la arquitectura de red. En particular se introduce la separación lógica de **los sistemas y redes de administración de otros sistemas y redes de información**, así como el despliegue de soluciones de detección y eliminación de softwares maliciosos y no autorizados.

- El TSP deberá optimizar los mecanismos de monitorizacion de sus sistemas, con el fin de detectar posibles incidentes de seguridad y responder en consecuencia mediante la implantación de herramientas y procesos que permitan la supervisión y el registro continuos de las actividades en la red y los sistemas de información de la entidad.

- El TSP deberá establecer procesos para la gestión de crisis que aborden como mínimo los aspectos siguientes:

- funciones y responsabilidades en situaciones de crisis;
- comunicaciones obligatorias y voluntarias entre el TSP y las autoridades competentes pertinentes, y
- controles adecuados para mantener la seguridad de la red y de la información en situaciones de crisis.

- El TSP deberá implantar un **proceso para gestionar y utilizar la información recibida del CSIRT nacional** o, en su caso, de las autoridades competentes que resulte útil para la gestión de crisis.

- El TSP deberá establecer un **procedimiento** sencillo **que permita a su personal, contratistas y clientes informar de posibles incidentes de seguridad** de la red y de la información. Dicho procedimiento deberá ser comunicado a sus contratistas y clientes.

- Las obligaciones de notificación de incidentes en virtud del artículo 19 de eIDAS quedan derogadas y la notificación de incidentes seguirá las directrices y el proceso definido en la Directiva NIS2 a partir del 17 de octubre de 2024. En particular se introduce como novedad lo siguiente:

- El TSP debe notificar a las autoridades competentes o al CSIRT cualquier incidente que tenga un "impacto significativo" en la prestación de sus servicios;

- Cuando proceda, el TSP debe incluir información sobre posibles repercusiones transfronterizas del incidente o si este responde a una acción ilícita o malintencionada;

- Los plazos para la notificación de los incidentes comprenden:

  - Alerta temprana (24 horas desde que se tuvo constancia de la ocurrencia del incidente); Esta respuesta incluirá, en particular sus comentarios iniciales sobre el incidente significativo y, a instancias de la entidad, una orientación o asesoramiento operativo sobre la aplicación de posibles medidas paliativas.

  - Informe de situación (si es requerido por el CSIRT o por la autoridad competente con la actualización de la gestión del incidente);

  - Informe final (1 mes a partir de que hayan gestionado el incidente).

- Cuando proceda, el TSP debe informar a las partes interesadas sobre los incidentes de seguridad y ciberamenazas que afecten al servicio y su gestión por la organización. Al respecto, el estándar ETSI estipula como novedad que los planes de comunicación desplegados deben incluir la categorización de incidentes, procedimientos de escalada bien definidos y protocolos normalizados para informar a las partes interesadas de la gestión del incidente.

- El TSP deberá identificar e implementar procesos y procedimientos para abordar los riesgos de seguridad asociados al uso de productos y servicios suministrados por proveedores, incluida la cadena de suministro de TIC.

- El TSP deberá definir, documentar e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados al uso de los productos o servicios del proveedor. En particular:

  - La política de la cadena de suministro deberá identificar y comunicar el papel del TSP en la cadena de suministro.

  - La política de la cadena de suministro deberá definir los criterios de selección y contratación de proveedores o prestadores de servicios. Los criterios deberán incluir:

    - la capacidad del proveedor o prestador de servicios para cumplir las especificaciones de ciberseguridad, los riesgos y los niveles de clasificación de los servicios, sistemas o productos del TSP suministrados por el proveedor o prestador de servicios;

    - la capacidad del TSP para diversificar las fuentes de suministro y limitar la dependencia de los proveedores; y

    - los resultados de las evaluaciones coordinadas de los riesgos para la seguridad de las cadenas de suministro críticas.

- El TSP deberá exigir que los proveedores de servicios de TIC **propaguen los requisitos de seguridad del TSP a lo largo de la cadena de suministro** si subcontratan partes del servicio de TIC prestado al TSP.

A efectos del artículo 23 de la Directiva NIS2 un incidente se considerará significativo si: a) ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada; b) ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

En principio, **a partir del 28 de febrero de 2025 puede ser exigible el cumplimiento de estos requisitos para todos los Prestadores de Servicios Electrónicos de Confianza,** que es la fecha prevista de aprobación de esta norma técnica, así como la fecha de retirada de cualquier norma nacional que puedan entrar en conflicto con ella.

En definitiva, la norma técnica ETSI EN 319 401, versión 3.1.1 (2024-06), aborda los requisitos generales para la gestión de seguridad y ciberseguridad de los servicios de confianza (tanto cualificados como no cualificados). La adaptación de las obligaciones y controles derivados de NIS2 a todos los prestadores cualificados de servicios electrónicos de confianza en la Unión Europea tiene implicaciones significativas, y garantiza una mayor seguridad y confiabilidad en la prestación de servicios, fortaleciendo el crecimiento del sector y beneficiando a la economía en general. Además, al aplicar medidas más robustas, se promueve la idea de un mercado único, permitiendo a los prestadores ofrecer sus servicios en cualquier país sin limitaciones.

En ECIJA, nuestro equipo de expertos está preparado para ayudar a los Prestadores de Servicios de Confianza a cumplir con las obligaciones de la Directiva NIS2 y la norma ETSI 319 401 y asesorarles en cada etapa de este proceso crucial. Ofrecemos servicios especializados para guiar a su organización en el proceso de adecuación, fortaleciendo sus medidas de ciberseguridad y garantizando el cumplimiento de la normativa europea.

Área de Privacidad y Protección de Datos de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60

Calle Serrano, 69.
28006 Madrid
www.ecija.com