ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

Nota informativa: Reglamento Europeo de Ciberseguridad

Madrid, 19 de junio de 2019

El pasado 7 de junio de 2019 se publicó el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019, relativo a ENISA (La Agencia de la Unión Europea para la Ciberseguridad), y a la certificación de la ciberseguridad de las tecnologías de la información ("Reglamento de Ciberseguridad").

Los principales objetivos de este Reglamento son la definición de las nuevas funciones de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), que verá fuertemente reforzadas sus capacidades, así como la creación de un sistema común de certificación en materia de seguridad de la información.

Agencia de la Unión Europea para la Cibereseguridad

La Unión Europea se enfrenta a un cambio de paradigma; la incipiente llegada de nuevos retos tecnológicos, la aparición de la era del internet de las cosas, así como de nuevas formas de comunicación ponen en jaque la seguridad de las redes haciendo que puedan verse afectadas por los ciberincidentes, los cuales, además de ser cada día más frecuentes y difíciles de atajar, **pueden producir importantes pérdidas económicas**. Esta nueva situación provoca que **la ciberseguridad sea una preocupación de primer nivel para la Unión Europea**.

Este nuevo panorama, ocasiona que las competencias de ENISA se vean considerablemente reforzadas con este nuevo Reglamento, así en el Art. 3, se define el mandato de ENISA, que pasará a tener carácter permanente, **configurando a la institución como punto de referencia de asesoramiento y conocimientos especializados en cuestiones relacionadas con la seguridad de la información** y las comunicaciones, las instituciones, órganos y organismos de la Unión, con el fin de lograr un elevado nivel de ciberseguridad común en toda la Unión, especialmente mediante el apoyo activo a los Estados miembros, a las instituciones, órganos y organismos de la Unión en la mejora de la ciberseguridad.

Creación de un marco común de certificación de ciberseguridad.

Uno de los puntos más importantes de este Reglamento es la **creación de un entorno común de certificación de ciberseguridad** que permita que, una vez emitida, esta sea reconocida de manera automática por todos los Estados Miembros.

La certificación desempeña un papel fundamental en el aumento de la seguridad de los productos y servicios que son cruciales para el desarrollo tecnológico de la Unión Europea. La situación actual del mercado interior se basa en la existencia de diferentes esquemas de certificación en materia de ciberseguridad, esta situación provoca la carencia de un marco común válido en todo el territorio comunitario, propiciando la aparición de un modelo altamente ineficiente para el propio funcionamiento de la Unión, ya que ocasiona barreras en nuestro bien más preciado: el mercado único comunitario.

Para paliar esta situación, este nuevo Reglamento proporcionará un conjunto de reglas, requisitos técnicos, estándares y procedimientos implementando un entorno único de certificación a nivel comunitario, lo que se traducirá en que **un certificado emitido por un Estado Miembro, sea automáticamente reconocido por todos los demás, facilitando el comercio trasfronterizo de las empresas y sus compradores al armonizar las características de seguridad del producto o servicio**.

Estos esquemas deberán tener al menos cubiertos los siguientes objetivos de seguridad;

- proteger los datos almacenados, transmitidos o tratados de otro modo frente al almacenamiento, tratamiento, acceso o revelación accidentales o no autorizados durante todo el ciclo de vida del producto, servicio o proceso de TIC;
- proteger los datos almacenados, transmitidos o tratados de otro modo frente a la destrucción accidental o no autorizada, la pérdida o la alteración o la falta de disponibilidad durante todo el ciclo de vida del producto, servicio o proceso de TIC;
- que las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiere su derecho de acceso;
- detectar y documentar las dependencias y vulnerabilidades conocidas;
- registrar qué datos, servicios o funciones han sido objeto de acceso, de uso o de otro tratamiento, en qué momentos y por quién;
- que sea posible comprobar qué datos, servicios o funciones han sido objeto de acceso, de uso o de otro tratamiento, en qué momentos y por quién;
- verificar que los productos, servicios y procesos de TIC no contengan vulnerabilidades conocidas;
- restaurar la disponibilidad y el acceso a los datos, servicios y funciones de forma rápida en caso de incidente físico o técnico;
- que los productos, servicios y procesos de TIC sean seguros por defecto y desde el diseño;
- que los productos, servicios y procesos de TIC se entreguen siempre con un programa informático y un equipo informático actualizados que no contengan vulnerabilidades conocidas públicamente, y dispongan de mecanismos para efectuar actualizaciones de seguridad.

El uso de los esquemas de certificación tendrá carácter voluntario, no obstante, **el uso de dichos esquemas podrá convertirse en una clara ventaja para aquellas empresas que deseen asegurar a los consumidores que sus productos y servicios se encuentran en cierto nivel de seguridad cibernética**. Dicho esquema fomenta así la llamada "seguridad por diseño". Adicionalmente, los fabricantes, distribuidores y proveedores también resultarán beneficiados, ya que un producto, verá agilizado considerablemente su llegada al mercado al evitar tener que pasar por varios procesos de certificación para conseguir la conformidad con el nivel de garantía de evaluación buscado, además, también los gobiernos se verán beneficiados, ya que podrán adoptar decisiones de compra más informadas identificando con mayor facilidad las áreas prioritarias para establecer la certificación de ciberseguridad,

En este sentido, cabe hacer referencia a la situación futura a la que se enfrenta el mecanismo de certificación del ENS español, ya que nuestro territorio es un claro caso de estado con un mecanismo de certificación a nivel nacional. Según este Reglamento, **en el momento que se apruebe un esquema de certificación que impacte en el mismo ámbito de uno nacional, este último dejará de surtir efecto de manera inmediata, según lo dispuesto en los arts. 49.7 y 57 del presente Reglamento**.

Esta convivencia entre ambos ecosistemas de certificaciones (el europeo y el nacional) van a hacer que sea importante tener en cuenta el ámbito de cada producto y servicios para determinar su afectación por dichos esquemas de certificación.