Deloitte.

Reglamento sobre la Ciberseguridad

Construcción del liderazgo europeo en ciberseguridad

Cyber

Introducción

El incremento de las ciberamenazas, la mejora en la sofisticación de los ciberataques, y el aumento del número de ciberincidentes está provocando un aumento de la sensación del nivel de ciberriesgo por parte de toda la sociedad, a la vez que incrementa la sensibilización de las empresas y las personas en la relevancia de mantener un entorno seguro. Esto ha influido en el aumento de la presión regulatoria a nivel europeo en materia de ciberseguridad, tanto a nivel sectorial como general.

Entre estas regulaciones, cabe destacar el **REGLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) nº 526/2013 («Reglamento sobre la Ciberseguridad»).** Este Reglamento, junto a la Directiva NIS, que ha sido transpuesta al ordenamiento jurídico español en septiembre de 2018, sientan las bases para proteger a las empresas y a la sociedad desde el punto de vista de ciberseguridad.

El Reglamento sobre la Ciberseguridad se centra en dos ámbitos bien diferenciados en el documento que se exponen a continuación:

- Una primera parte que tiene como objetivo la potenciación de la ENISA (Agencia de la Unión Europea para la Ciberseguridad), de forma que se establecen los objetivos, tareas y aspectos organizativos de la misma.

- Una segunda parte que tiene como objetivo establecer un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de TIC en la Unión, así como de evitar la fragmentación del mercado interior respecto a los esquemas de certificación de la ciberseguridad en la Unión.

El presente artículo tiene como objetivo resumir los principales aspectos de este Reglamento, haciendo especial hincapié especial en lo relativo al marco para la creación de esquemas de certificación. De esta manera, se pretende contestar a las siguientes preguntas:

1. **¿Cómo será la futura ENISA?**
2. **¿Qué objetivos persigue el marco para la creación de esquemas europeos?**
3. **¿Qué elementos pueden verse afectados por este marco?**
4. **¿Qué organismos están involucrados en la aplicación de este marco?**
5. **¿Qué requisitos cumplen los esquemas de certificación?**
6. **¿Qué información adicional debe proporcionar el fabricante o proveedor?**
7. **¿Existe un régimen sancionador?**
8. **¿Cuáles son los próximos pasos?**

1. Futura Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Uno de los principales aspectos de este Reglamento es el de potenciar una Agencia de la Unión Europea para la Ciberseguridad que ayude al desarrollo del sector de la ciberseguridad, de forma que pueda afrontarse el aumento de las ciberamenazas y los ciberataques de una forma coordinada.

La ENISA desempeñará un conjunto de actividades con el fin de lograr un elevado nivel de ciberseguridad común, que permita reducir asimismo la fragmentación del mercado interior. Para ello, el Reglamento define los objetivos que tendrá la futura ENISA, así como las tareas que se le encomiendan para poder conseguir y lograr dichos objetivos:

Objetivos

- Ser un centro de conocimientos técnicos sobre ciberseguridad.
- Asistir a las instituciones, órganos y organismos de la Unión en la elaboración y aplicación de políticas de la Unión en materia de ciberseguridad.
- Prestar su apoyo a la creación de capacidades y a la preparación de toda la Unión.
- Fomentar la cooperación entre los Estados miembros y diferentes organismos.
- Contribuir a incrementar las capacidades de ciberseguridad.
- Promover el uso de la certificación europea de ciberseguridad.
- Promover un alto nivel de sensibilización.

Tareas

- Contribución a la elaboración y ejecución de la Política y el Derecho de la Unión.
- Creación de capacidades, asistiendo a los Estados miembro en la incorporación de esas capacidades o necesidades que puedan tener.
- Cooperación operativa a nivel de la Unión, apoyando la cooperación entre Estados, instituciones, órganos, organismos y partes interesadas, buscando sinergias entre todos ellos.
- Fomento del mercado de ciberseguridad en la Unión, apoyando y promoviendo la aplicación de los esquemas de certificación de ciberseguridad.
- Conocimiento e información, efectuando análisis de tecnologías, preparando evaluaciones, realizando análisis estratégicos y, en definitiva, poniendo a disposición del público información sobre la ciberseguridad.
- Sensibilización y educación, trasladando buenas prácticas y asistiendo a los Estados miembros en lo que necesiten.
- Investigación e innovación, asesorando sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad y contribuyendo a fijar la agencia estratégica de investigación e innovación.
- Cooperación internacional, contribuyendo para cooperar con terceros países y organizaciones internacionales.

Para esto, se ha establecido una estructura administrativa y de gestión de la ENISA, compuesta por los siguientes elementos:

Consejo de administración

- Definirá la orientación general y velará por que se trabaje con las normas y principios establecidos.
- Se reunirá al menos dos veces al año en sesión ordinaria.

Comité ejecutivo

- Asistirá al Consejo de Administración y se encargará de garantizar un seguimiento adecuado de las conclusiones y recomendaciones, y asistirá al Director Ejecutivo en cuestiones administrativas y presupuestarias.
- Se reunirá al menos una vez cada tres meses.

Director ejecutivo

- Gestionará la ENISA, actuando con independencia, dando cuenta de su gestión al Consejo de Administración, informando al Parlamento Europeo sobre el ejercicio de sus funciones, y también al Consejo cuando sea convocado.
- Como parte de esta gestión, se llevará a cabo la administración ordinaria, la ejecución de las decisiones del Consejo de Administración, etc.

Grupo Consultivo de ENISA

- Estará compuesto por expertos reconocidos (representantes de industria de las TIC, proveedores de redes o servicios de comunicaciones electrónicas, pymes, etc.).
- Será establecido por el Consejo de Administración a propuesta del Director Ejecutivo.
- Asesorará en la elaboración del programa de trabajo anual y en el mantenimiento de la comunicación con las partes interesadas.

Grupo de las Partes Interesadas sobre Certificación de la Ciberseguridad

- Estará compuesto por expertos reconocidos que se encargarán de asesorar a ENISA y a la Comisión sobre aspectos relacionados con el marco europeo de certificación de la ciberseguridad.

Red de funcionarios de enlace nacionales

- Será establecida por el Consejo de Administración, a propuesta del Director Ejecutivo.
- Estará compuesta por representantes de los Estados miembros.
- Se encargarán de facilitar el intercambio de información entre Estados miembro y ENISA.

2. ¿Qué objetivos persigue el marco para la creación de esquemas europeos de certificación de la ciberseguridad?

El establecimiento de un marco europeo para la certificación de ciberseguridad persigue, entre otros, los siguientes objetivos:

- Mejorar las condiciones de funcionamiento del mercado interno elevando el nivel de ciberseguridad en la Unión.
- Establecer los mecanismos para habilitar esquemas de certificación en ciberseguridad a nivel europeo.
- Facilitar la creación del mercado único digital para procesos, productos y servicios TIC.
- Establecer los requerimientos que deben cumplirse con el objetivo de proteger la disponibilidad, autenticidad, integridad y confidencialidad de: (1) los datos almacenados, transmitidos o procesados; (2) las funciones y servicios ofrecidos por (o accesibles a través de) esos productos, procesos y servicios.

Todo esto facilitará la disminución del ciberriesgo de los productos, servicios y procesos TIC en toda la Unión Europea, aumentando con ello la confianza de los usuarios y empresas, fomentando así el uso de los mismos.

3. ¿Qué elementos se verán afectados por el marco establecido?

Los futuros esquemas que se definirán bajo el amparo de este Reglamento sobre la Ciberseguridad afectarán, como se ha introducido anteriormente, a productos, servicios y procesos TIC, siendo dichos esquemas aplicables a nivel europeo.

A este respecto cabe destacar que se establecerá un programa de trabajo evolutivo de la Unión que fijará las prioridades estratégicas para los futuros esquemas de certificación, de forma que se podrá saber, de antemano y salvo excepciones, cuáles serán los futuros esquemas que se construirán para así poder anticiparse.

Asimismo, en este programa se incluirán una lista de productos, servicios y procesos TIC (o categorías de los mismos) que podrían ser incluidos en el ámbito de aplicación de un esquema, facilitando así su identificación.

Este primer trabajo evolutivo se publicará como tarde el 10 de junio de 2020, y se actualizará al menos cada 3 años.

Productos TIC

Un elemento o un grupo de elementos de las redes y los sistemas de información

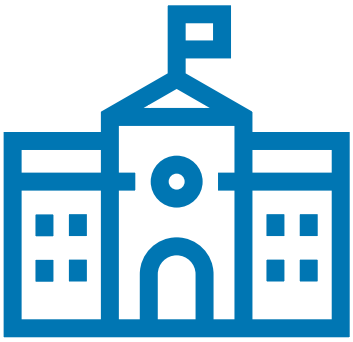
Servicios TIC

Un servicio que consista, en su totalidad o principalmente, en la transmisión, almacenamiento, extracción o tratamiento de información mediante redes y sistemas de información

Procesos TIC

Un conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC

4. ¿Qué organismos están involucrados en la aplicación del marco?



Como parte del marco se incluyen múltiples organismos que tendrán un conjunto de responsabilidades y acciones a acometer. A continuación, se recogen algunos de los principales, junto a sus tareas más significativas:

ENISA

- Preparará las propuestas de esquemas de certificación de ciberseguridad europeos, para lo cual podrá consultar a todas las partes interesadas, a través de un proceso de consulta oficial transparente e inclusivo.
- Evaluará al menos cada cinco años los esquemas teniendo en cuenta los comentarios recibidos de las partes interesadas.
- Mantendrá un sitio web para ofrecer información sobre los esquemas europeos de certificación de la ciberseguridad, los certificados europeos y las declaraciones de conformidad. Este sitio incluirá asimismo aquellos certificados que no son válidos o han sido retirados o caducados, y también reflejará los esquemas nacionales que han sido sustituidos por esquemas europeos.

Grupo Europeo de Certificación de la Ciberseguridad (CEGG)

- Asistirá, cooperará y aconsejará a la ENISA en la preparación de los esquemas de certificación de ciberseguridad europeos.
- En casos debidamente justificados, podrá solicitar a ENISA que prepare una propuesta de esquema o que revise un esquema europeo de certificación de la ciberseguridad existente que no esté incluido en el programa de trabajo evolutivo de la Unión.

Comisión Europea

- Podrá adoptar los esquemas de certificación, a través de actos de ejecución.
- Podrá solicitar a ENISA que prepare una propuesta de esquema o que revise un esquema europeo de certificación de la ciberseguridad basándose en el programa de trabajo evolutivo de la Unión. También podrá solicitarlo si no está dentro del programa evolutivo en casos debidamente justificados.
- Evaluará periódicamente la eficacia y la utilización de los esquemas europeos de certificación, así como si debe convertirse en obligatorio (la primera vez, antes del 31 de diciembre de 2023, y después cada 2 años).

Estados miembros

- Designarán una o más autoridades nacionales de certificación.
- Establecerán el régimen de sanciones aplicables a los incumplimientos (efectivas, proporcionadas y disuasorias).

Autoridades nacionales de certificación y Organismos de evaluación de la conformidad

- Certificarán productos, servicios y procesos TIC.

5. ¿Qué requisitos cumplen los esquemas de certificación?

Los esquemas de certificación serán voluntarios, salvo que una legislación futura de la Unión Europea o de los Estados miembros establezca que debe ser obligatoria para cumplir con alguna necesidad. De esta manera, podrán existir ciertos esquemas de certificación de obligado cumplimiento para un conjunto específico de elementos.

Las certificaciones serán reconocidas en todos los Estados miembros, dando fe del cumplimiento de los requisitos exigidos en el correspondiente esquema. De hecho, estas certificaciones a nivel europeo primarán sobre posibles esquemas nacionales de certificación, de forma que algunos de ellos podrían verse impactados, y dejar de ser de aplicación en caso de que se apruebe un esquema de certificación a nivel europeo que tenga el mismo ámbito de actuación. Es por ello que habrá que estar especialmente atentos a aquellos esquemas de certificación a nivel nacional que están en vigor o en fase de construcción (certificación ENS, futura certificación CNPIC, etc.), para saber finalmente en qué situación quedan.

En cuanto a la estructura de los esquemas de certificación, se establecerán tres niveles de garantía: básico, sustancial y elevado.

Básico

- Ofrece garantías de que los productos, servicios y procesos TIC cumplen con los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos básicos conocidos de ciberincidentes o ciberataques.
- La evaluación incluye al menos una revisión de la documentación técnica.
- Podría permitirse la obtención mediante una autoevaluación, a través de una declaración de conformidad que les hace responsable.

Sustancial

- Ofrece garantías de que los productos, servicios y procesos TIC cumplen con los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar los riesgos relacionados con la ciberseguridad conocidos, los riesgos de incidentes y los ciberataques cometidos por agentes con capacidades y recursos limitados.
- La evaluación incluye al menos la revisión para demostrar la ausencia de las vulnerabilidades conocidas públicamente y la comprobación de que los productos, servicios o procesos TIC aplican correctamente las funcionalidades de seguridad necesarias.

Elevado

- Ofrece garantías de que los productos, servicios y procesos TIC cumplen con los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad, y de que se han evaluado hasta un nivel que pretende minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables.
- La evaluación incluye, al menos la revisión de improcedencia de vulnerabilidades conocidas públicamente, la comprobación de que aplican correctamente la funcionalidad de seguridad (con las tecnologías mas avanzadas), y la evaluación de resistencia a través de pruebas de penetración.

6. ¿Qué objetivos se persiguen con los esquemas de certificación?

Los esquemas de certificación se diseñarán para cumplir con unos objetivos que ya están definidos en el propio Reglamento, de forma que permitan cubrir los distintos aspectos de ciberseguridad que pueden afectar a un producto, servicio o proceso TIC:

Proteger los datos frente a almacenamiento, tratamiento o acceso no autorizado

Proteger los datos frente a destrucción, pérdida o falta de disponibilidad

Acceder exclusivamente a los datos, servicios y funciones según su derecho de acceso

Detectar y documentar dependencias y vulnerabilidades conocidas

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 no existen vulnerabilidades conocidas

Restaurar la disponibilidad y acceso de forma rápida en caso de incidente

Entregar con programas y equipos actualizados, sin vulnerabilidades y que puedan ser actualizados periódicamente

Establecer la seguridad por diseño y por defecto

7. ¿Qué información adicional debe proporcionar el fabricante o proveedor?

Además de la certificación que debe obtenerse, el fabricante o proveedor debe aportar un conjunto de información que permita a los usuarios mantener el nivel de seguridad en el uso de los distintos elementos, entre los que se deben incluir, al menos, los siguientes puntos:

Orientaciones y recomendaciones para ayudar a los usuarios finales con la configuración, la instalación, el despliegue, el funcionamiento y el mantenimiento seguros de los productos o servicios de TIC

El periodo durante el cual se ofrecerá a los usuarios finales apoyo en materia de seguridad, en particular en lo que se refiere a la disponibilidad de actualizaciones relacionadas con la ciberseguridad

Datos de contacto del fabricante o proveedor y métodos aceptados para recibir información sobre vulnerabilidades de usuarios finales o investigadores en materia de seguridad

Una referencia a los registros en línea en los que consten las vulnerabilidades conocidas públicamente en relación con el producto, servicio o proceso de TIC, así como recomendaciones pertinentes en materia de ciberseguridad

Además, aunque se haya obtenido el certificado para un producto, servicio o proceso, los fabricantes y proveedores deberán informar a la autoridad u organismo de cualquier vulnerabilidad o irregularidad detectada posteriormente a la obtención del mismo, sin demora indebida.

Esto permite que, con la debida diligencia de los fabricantes y proveedores, las autoridades de certificación tengan el conocimiento necesario para poder tomar decisiones sobre las certificaciones ya entregadas sin necesidad de esperar al plazo de renovación del certificado.

8. ¿Existe un régimen sancionador?

El Reglamento no establece un régimen sancionador, pero sí que prevé la posible existencia del mismo. Cabe destacar que, aunque los esquemas de certificación sean de aplicación a nivel europeo, el Reglamento establece que serán los Estados miembros quienes tendrán que establecer el régimen de sanciones aplicables a los incumplimientos, aunque siempre destacando que deben ser efectivas, proporcionadas y disuasorias.

Conclusiones

El presente Reglamento continúa con el camino iniciado por la Unión Europea en incrementar las capacidades de ciberseguridad dentro de la Unión, fortaleciendo a la ENISA y estableciendo las bases para la creación de esquemas de certificación en ciberseguridad.

Esto favorecerá el desarrollo del Mercado Único Digital, si bien el éxito de los esquemas de certificación, al no existir un régimen sancionador, dependerá de las ventajas percibidas por las organizaciones de adherirse a dichos esquemas. Esto a su vez estará ligado al aumento de la sensibilización que el consumidor en relación a un producto, servicio o proceso certificado respecto a otro sin el sello de certificación.

Respecto a la implantación de los esquemas, una de las preocupaciones que pueden surgir es una potencial diferencia de criterios entre las diferentes autoridades nacionales de certificación. Para ello, se ha habilitado dentro del propio Reglamento la posibilidad de revisiones interpares entre dichas autoridades, lo que permite garantizar unas normas equivalentes entre ellas, reduciendo las opciones de que se puedan seleccionar autoridades nacionales de certificación donde sea más fácil conseguir dichas certificaciones.

De la misma forma, otra de las preocupaciones que debe tenerse en cuenta es la potencial falsa sensación de seguridad que se puede tener por parte de los usuarios al disponer de un producto, servicio o proceso etiquetado con una certificación concreta. Es por ello que, pese a la creación de estos esquemas de certificación, se seguirá identificando como una de las partes más importantes de la ciberseguridad la concienciación y sensibilización del usuario. De esta forma, a pesar de tener elementos certificados con un nivel de seguridad determinada, deben seguir usándose teniendo en cuenta las mejores prácticas para evitar potenciales riesgos.

Próximos pasos

Una vez que ha entrado en vigor el Reglamento, deben definirse los esquemas de certificación a los que es posible adherirse. Además de esto, dentro del propio Reglamento se han establecido distintas fechas en las que deben cumplirse un conjunto de hitos:

28/12 2019

- El Consejo de Administración adoptará disposiciones para la aplicación del Reglamento (CE) nº 1049/2001, relativa al acceso del público a los documentos del Parlamento Europeo.
- Con el fin de facilitar la lucha contra el fraude, la corrupción y otras actividades ilegales con arreglo al Reglamento (UE, Euratom) nº 883/2013 del Parlamento Europeo y del Consejo, ENISA suscribirá el Acuerdo Interinstitucional, de 25 de mayo de 1999, entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión de las Comunidades Europeas, relativo a las investigaciones internas efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF), y adoptará las disposiciones apropiadas, que serán de aplicación a todo el personal de ENISA, sirviéndose del modelo contenido en el anexo de dicho Acuerdo.

10/06 2020

- Fecha límite para publicar el primer programa de trabajo evolutivo de la Unión.

28/06 2021

- Los artículos 58, 60, 61, 63, 64 y 65 comienzan a ser de aplicación. Estos artículos son relativos a las autoridades nacionales de certificación, los organismos de evaluación de la conformidad, las notificaciones asociadas, el derecho a presentar una reclamación y a la tutela efectiva, así como la potestad de los Estados miembros de establecer el régimen sancionador.

21/12 2024

- Fecha límite para la evaluación por parte de la Comisión del impacto, la eficacia y la eficiencia de la ENISA y sus prácticas de trabajo, junto a la posible necesidad de modificar su mandato y las repercusiones financieras que tendría la eventual modificación; así como para la emisión del informe al Parlamento Europeo, al Consejo y al Consejo de Administración.

Anexo: ¿Qué contendrá, al menos, un esquema de certificación?

El artículo 54 del Reglamento de Ciberseguridad establece que los esquemas de certificación incluirán al menos los siguientes elementos:

- Objeto y alcance.
- Finalidad.
- Referencias.
- Niveles de garantía.
- Autorización para autoevaluación.
- Requisitos de organismos de evaluación de conformidad.
- Criterios y métodos de evaluación específicos.
- Información necesaria.
- Condiciones de uso de etiquetas o marcas.
- Normas para controlar el cumplimiento.
- Condiciones de expedición, mantenimiento, renovación y modificación del alcance.
- Consecuencias para aquellos que no cumplan los requisitos.
- Normas para notificar vulnerabilidades no detectadas previamente.
- Normas para conservación de registros por organismos de evaluación.
- Esquemas nacionales o internacionales que cubren aspectos similares.
- Contenido y formato de certificados.
- Periodo de disponibilidad de la declaración de conformidad de la UE, documentación técnica y otra información pertinente.
- Periodo máximo de validad de certificados.
- Política de divulgación de certificados.
- Condiciones de reconocimiento mutuo.
- Normas relativas a mecanismos de evaluación interpares.
- Formato y procedimientos para proporcionar y actualizar información complementaria.

Deloitte.

Diseñado y producido por el Dpto. de Marketing & Brand.