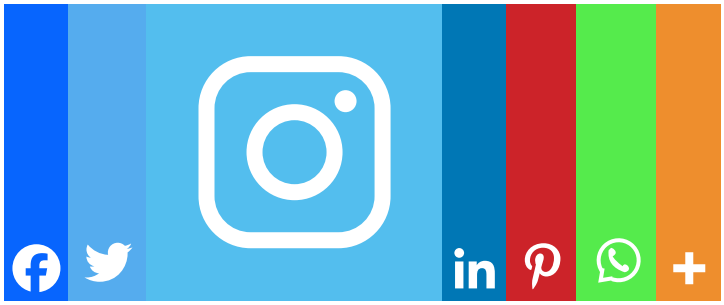
Spread the love



Pelargonium hortorum (geranio rojo)

Con el desarrollo de la certificación de ciberseguridad a escala de la UE se pretende armonizar el reconocimiento del nivel de ciberseguridad de las soluciones TIC en toda la Unión.

Los sistemas de certificación de la UE son desarrollados por ENISA dentro del marco definido en el Reglamento sobre Ciberseguridad (Reglamento 881 /2019), y constituyen un mecanismo europeo principal para ir generando un ámbito europeo ciberseguro

Definición de Esquema europeo de certificación de la ciberseguridad de la UE: es un conjunto completo de reglas, requisitos técnicos de ciberseguridad, normas y procedimientos de evaluación, definidos a nivel de la UE y aplicables a la certificación de productos, servicios o procesos específicos de TIC.

- Cada certificado de ciberseguridad de la UE de un Esquema Europeo de Certificación de la Ciberseguridad acredita que un producto, proceso o servicio de TIC ha superado una evaluación de conformidad con dicho régimen y que cumple los requisitos y normas de ciberseguridad especificados en el propio esquema.
- La certificación la realiza un *organismo de evaluación de la conformidad* (OEC/CAB), que puede auditar y/o probar y/o certificar.

- Todos los certificados serán publicados por ENISA en un sitio web específico.
- Dependiendo del riesgo de ciberseguridad asociado al uso previsto de la solución TIC que se va a certificar, se puede elegir un nivel de ciberseguridad diferente Cada esquema indica si la certificación tiene un nivel de garantía «básico», «sustancial» o «alto»

Los esquemas europeos de ciberseguridad se irán aprobando son -en principio- voluntarios. Su seguimiento potencia el Mercado Único Digital de la UE. Sirven para demostrar el cumplimiento de requisitos de ciberseguridad. En algunos casos, cuando pueden llegar a ser obligatorios.

Alguna legislación ya alude a los esquemas europeos de certificación de ENISA. Por ejemplo:

- – la Directiva para un alto nivel de ciberseguridad en toda la Unión (NIS2), en especial en lo relativo a entidades que gestionan infraestructuras críticas. Y, en su considerando 80 se indica: «*Con el fin de demostrar el cumplimiento de las medidas para la gestión de riesgos de ciberseguridad y en ausencia de esquemas europeos de certificación de la ciberseguridad adecuados que se hayan adoptado de conformidad con el Reglamento (UE) 2019/881 ,…, los Estados miembros, consultando (…) deben promover el uso de las normas europeas e internacionales pertinentes por parte de las entidades esenciales e importantes, o pueden exigir a las entidades que utilicen productos, servicios y procesos de TIC certificados».*
- El Reglamento de Ciberresiliencia (CRA), que añade la ciberseguridad a los criterios para obtener el marcado CE en la fabricación de determinados productos

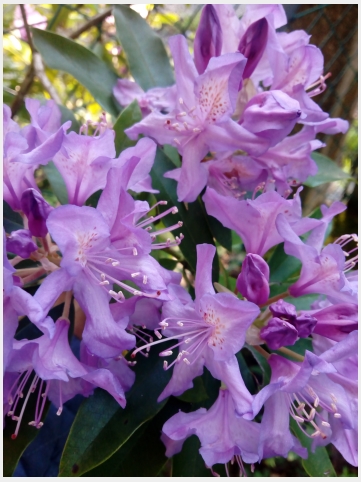
Definición de Esquema europeo de certificación de la ciberseguridad de la UE: es un conjunto completo de reglas, requisitos técnicos de ciberseguridad, normas y procedimientos de evaluación, definidos a nivel de la UE y aplicables a la certificación de

productos, servicios o procesos específicos de TIC.

- Cada certificado de ciberseguridad de la UE acredita que un producto, proceso o servicio de TIC ha superado una evaluación de conformidad con dicho régimen y que cumple los requisitos y normas de ciberseguridad especificados.
- La certificación la realiza un organismo de evaluación de la conformidad (OEC/CAB), que puede auditar y/o probar y/o certificar. Todos los certificados serán publicados por ENISA en un sitio web específico.
- Dependiendo del riesgo de ciberseguridad asociado al uso previsto de la solución TIC que se va a certificar, se puede elegir un nivel de ciberseguridad diferente que el solicitante define. Cada esquema indica si la certificación tiene un nivel de garantía «básico», «sustancial» o «alto»

Los primeros EEC::

- **EUCC.** El Esquema Europeo de Certificación de Ciberseguridad sobre Criterios Comunes, el primer esquema, se dirige a las TIC, tales como productos y componentes de hardware y software. El 31 de enero de 2024, la Comisión Europea aprobó el acto de ejecución por el que se pone en marcha el sistema de certificación. ENISA está publicando los documentos de referencia que respaldan el sistema y que se enumeran en su Anexo 1.



Rododendro

A continuación:

- **EUCS** El Esquema Europeo de Certificación de Servicios en la Nube se encuentra en trámite de análisis por parte del ECCG.
- **EU5G** El Esquema Europeo de Certificación de Ciberseguridad para 5G se desarrolla en dos fases.

Durante una primera fase que finalizó en otoño de 2022, ENISA, los expertos reunidos en un grupo de trabajo ad hoc con la Comisión de la UE y los Estados miembros analizaron las evaluaciones industriales existentes y los esquemas de certificación y sus actualizaciones necesarias para cumplir con la Ley de Ciberseguridad. La segunda fase se abre con una consulta pública

- **¿Inteligencia Artificial?** Con vistas a la adopción del proyecto de Reglamento de la UE sobre Inteligencia Artificial, ENISA está evaluando si la IA podría ser objeto de certificación en materia de ciberseguridad y de qué manera, así como el modo en que podrían reutilizarse los esquemas en curso de elaboración. Este trabajo es preparatorio, ya que ENISA no ha recibido una solicitud para desarrollar un esquema de certificación por parte de la Comisión Europea

Arquitectura en la elaboración y utilización de los EEC

Hortensia atlántica

- **Comisión Europea** La iniciativa de elaborar un EECC es de la Comisión Europea que lo plantea a ENISA. ENISA, una vez que tiene una propuesta, la remite a la Comisión quien la adopta a través de legislación administrativa, Reglamentos de Ejecución
- **ENISA.** La elaboración corresponde a ENISA que actúa como coordinadora y anfitriona de grupos de trabajo
- **Partes interesadas y público general** Al desarrollar los esquemas de ciberseguridad de la UE, ENISA trabaja con una amplia variedad de partes interesadas en la ciberseguridad. Por ejemplo, las partes interesadas pueden formar parte del «grupo

de trabajo ad hoc» de expertos que apoya a la ENISA en el desarrollo de un determinado esquema. Asimismo, es posible invitar a las partes interesadas a participar en proyectos piloto o «pruebas de concepto» para poner a prueba algunos o más elementos de un régimen de la UE (por ejemplo, viabilidad, posibles procedimientos o procesos o métodos de evaluación) antes de su aplicación. Por otro lado, cuando un esquema se encuentra en una fase avanzada de desarrollo, también puede haber consultas públicas, por ejemplo sobre proyectos de regímenes. Una vez implantado, el sistema debe actualizarse y adaptarse a los cambios que se produzcan en el entorno de la ciberseguridad. Los procesos, procedimientos y métodos de evaluación deben mantenerse, evaluarse y revisarse y en estos procesos también participan las partes interesadas por invitación de ENISA.

- **Entrada en vigor:** Para ser efectivo, un proyecto de esquema elaborado por ENISA a petición de la Comisión debe ser aprobado por un acto legislativo de la UE , «acto de ejecución» y en él se establece un periodo para que los Estados miembros preparen el funcionamiento del sistema antes de expedir los certificados.
- **Organismos de Evaluación de la Conformidad (OEC/CAB) .**Los OEC/CAB que estarán acreditados para emitir certificados o realizar actividades de evaluación (ensayos, auditorías) para estos esquemas.. Los sistemas de certificación de ciberseguridad crean un mercado europeo para organismos de evaluación de la conformidad (OEC/CAB) que podrán ofrecer sus servicios de certificación así como herramientas y servicios de evaluación relacionados en toda la UE. Estos OEC/CAB trabajan en los esquemas de certificación de la UE de dos formas distintas: como evaluadores (mediante

auditorías/ensayos) y/o como certificadores. Deben cumplir una serie de requisitos antes de poder realizar tales actividades:
– Para poder evaluar y certificar de acuerdo con los regímenes de certificación de la UE, los OEC deberán estar ***acreditados por su organismo nacional de acreditación.***
– Una vez acreditados para un esquema europeo de certificación de la ciberseguridad, la Autoridad Nacional de Certificación de la Ciberseguridad (ANC) deberá notificar su acreditación a la Comisión.
– Si un OEC quiere ser elegible para certificar una solución TIC bajo el nivel de garantía «alto», puede necesitar cumplir requisitos adicionales. ***El procedimiento para cumplir estos requisitos lo realiza la ANC y se denomina «autorización». Esta «autorización» también debe notificarse a la Comisión.***

- **Usuarios de los certificados** Los certificados de ciberseguridad de la UE se conceden a productos y servicios TIC certificados con arreglo a los regímenes de certificación de ciberseguridad de la UE. Demuestran que las soluciones probadas son resistentes a determinados niveles de seguridad y establecen procesos de reparación teniendo en cuenta los últimos avances del estado de la técnica. Como están reconocidos en toda la UE permiten a los proveedores de productos y servicios mostrar la conformidad de su solución con un esquema específico, nivel de garantía, ámbito de aplicación y, potencialmente, extensión o perfiles de seguridad. Los usuarios de soluciones TIC pueden considerar los certificados de ciberseguridad como una demostración de que una solución específica cumple los requisitos de seguridad definidos.
- **Autoridades Nacionales de Certificación en Ciberseguridad (ANC).** Como exige la Directiva sobre

Ciberseguridad, cada Estado miembro ha designado una ANC que se responsabilizará de supervisar, acreditar y controlar la certificación de ciberseguridad de la UE a nivel nacional y de intercambiarla a nivel de la UE. Cada Estado miembro puede optar por expedir certificaciones de conformidad de ciberseguridad de la UE. Las Autoridades Nacionales de Certificación en Ciberseguridad («ANC») supervisan y controlan el cumplimiento del régimen de los certificados expedidos por las OEC en su Estado miembro.

- **Sistemas nacionales.** Cada sistema de certificación de ciberseguridad de la UE prevé un periodo de transición tras el cual los sistemas nacionales pertinentes dejan de tener efecto. En otras palabras, los certificados expedidos en virtud de estos regímenes dejan de ser válidos. Para garantizar una aplicación sin problemas, la transición de los regímenes existentes a los regímenes de la UE se lleva a cabo en estrecha colaboración con todas las partes interesadas; por ejemplo, se elaborarán orientaciones para los organismos de certificación de ciberseguridad que operan con regímenes nacionales. Por lo tanto, los OEC no deben interrumpir sus actividades relacionadas con los regímenes existentes.
- **Duración.** Los certificados son válidos durante un tiempo limitado que puede ampliarse mediante una nueva evaluación de la solución.
- **Certificación** la certificación es voluntaria, a menos que la normativa de la UE o de los Estados miembros especifique lo contrario.

Investigación financiada por el proyecto nacional PID2021-127527OB-I00, Proyectos de Generación de Conocimiento 2021, Modalidades: Investigación No Orientada e Investigación Orientada