Contacto

Certificado de Conformidad de Ciberresiliencia

Prepárate para la nueva Ley de Ciberresiliencia (CRA) de la UE. Evalúa el nivel de adhesión a los requisitos esenciales de ciberseguridad de la CRA y mejora la madurez de ciberresiliencia de tus productos y de los procesos de su empresa. La Marca Applus+ de Ciberresiliencia permite evaluar la adhesión de los productos a los requisitos esenciales de la CRA (Cyber Resilience Act), para las categorías 'Default' o 'Unclassified'.

Se espera que el CRA entre en vigor en el segundo semestre de 2024, y los fabricantes dispondrán de 36 meses para aplicar la mayoría de sus requisitos, excepto la obligación de notificar incidentes y vulnerabilidades, que empezará antes. En este caso los fabricantes deberán a empezar reportar a los 21 meses de la entrada en vigor del CRA. La CRA afectará a una amplia gama de empresas que venden sus productos digitales en Europa, pero con diferentes grados de rigor. Lea nuestra publicación para conocer en profundidad los requisitos esenciales de la CRA y los productos afectados.

Todos los vendedores afectados por el nuevo reglamento deben empezar a prepararse, ya que el cumplimiento afectará al desarrollo del producto, y comenzar a evaluar la madurez de la empresa en el ámbito de la ciberresiliencia. Applus+ Laboratories ha desarrollado un nuevo Certificado de Conformidad dirigido a los proveedores de productos no críticos, calificados como 'Default' o 'Unclassified' según la definición de la CRA. Se espera que alrededor del 90% de los productos afectados por la CRA pertenezcan a esta categoría. Aunque estos proveedores pueden optar por una autoevaluación, el cumplimiento de los requisitos de la CRA será una obligación legal, incluida la presentación de todas las evidencias necesarias (con posibles multas para las empresas que no cumplan).

Metodología de evaluación de la ciberresiliencia

Applus+ Laboratories ha desarrollado una metodología interna, asentada en la metodología europea de evaluación de la ciberseguridad a tiempo fijo para productos TIC (FITCEM) EN 17640:2022.

FITCEM EN 17640:2022 es un marco genérico para desarrollar metodologías de evaluación basadas en un conjunto de tareas predefinidas. Fue desarrollada por CEN CENELEC para estandarizar metodologías nacionales existentes como LINCE (España), CSPN (Francia) o BSZ (Alemania) con la participación de expertos de Applus+ Laboratories como coeditores. Nuestra metodología interna en una instanciación de FITCEM, adaptada a los futuros requisitos de la CRA. Nuestros expertos en diferentes tecnologías pueden analizar las necesidades específicas en función del tipo de producto.

Tareas de evaluación incluidas en el servicio y definidas en el FITCEM:

- Comprobación de integridad: una comprobación de integridad para revisar que Applus+ Laboratories recibe todas las pruebas solicitadas.
- Revisión de las funcionalidades de seguridad: se revisa la evaluación de análisis de riesgos obligatoria realizada por el fabricante para garantizar que las funcionalidades de seguridad están bien definidas y cubren los riesgos identificados por el fabricante.
- Documentación de desarrollo: se analizan los procesos y documentos proporcionados por el fabricante y se verifica el cumplimiento de los requisitos de la CRA en cuanto al tratamiento de productos y vulnerabilidades.
- Revisión de vulnerabilidades: se realiza una revisión del análisis de vulnerabilidades basado en vulnerabilidades públicas o conocidas para el producto y sus componentes.

Evidencias necesarias para el Certificado de conformidad de ciberresiliencia

El fabricante deberá aportar las siguientes evidencias, incluidas en el archivo técnico (ver Anexos II y V):

- **Descripción del producto**, incluida la identificación del producto y las funcionalidades de seguridad, manuales, directrices para el usuario, etc.
- Una **descripción del diseño** (especificaciones funcionales, algoritmos criptográficos, módulos, componentes...), los procesos de desarrollo y producción y los procesos de gestión de vulnerabilidades y gestión de parches.
- Una **evaluación de los riesgo**s de ciberseguridad frente a los que se diseña, desarrolla, produce, entrega y mantiene el producto con elementos digitales, tal como se establece en el artículo 10 de la CRA. Procedimientos de evaluación de riesgos y último análisis de riesgos.
- Si se aplican, una **lista de las normas armonizadas, especificaciones comunes y esquemas de ciberseguridad aplicado**s total o parcialmente. Si no se han aplicado

estas normas armonizadas, especificaciones comunes o regímenes de certificación de la ciberseguridad, descripciones de las soluciones adoptadas para cumplir los requisitos esenciales;
- **Informes de las ensayos realizados** para verificar la conformidad del producto y de los procesos de tratamiento de la vulnerabilidad con los requisitos esenciales aplicables, tal como se establece en las secciones 1 y 2 del anexo I de la CRA;
- Una copia de la **declaración UE de conformidad** (opcional, no necesaria para la presente evaluación);
- En su caso, la **lista de materiales del software**, tal como se define en el punto 36 del artículo 3 de la CRA.

¿Qué se obtiene?

El resultado de la evaluación es un CoC (Certificado de Conformidad) que enumera que requisitos se cumplen, tanto a nivel de producto y como de gestión de vulnerabilidades. El CoC irá acompañado del derecho a utilizar la marca 'Applus+ Cyber Resilience'.

¿Por qué elegir el CoC de Ciberresiliencia de Applus+?

En Applus+ Laboratories colaboramos con nuestros clientes en la construcción de un futuro digital ciberresiliente. Somos un laboratorio líder la certificación Common Criteria y expertos de primer nivel en evaluaciones de seguridad, con más de 20 esquemas de ciberseguridad para diferentes verticales, desde sistemas de pago a IoT, pasando por automoción o criptografía para la industria de defensa.

Adelántate a las próximas normativas de ciberseguridad

Tanto si tus productos se van a clasificar como Default, Class I o Class II, la marca de conformidad Applus+ Cyber Resilience:

- Muestra el compromiso de su organización con la ciberresiliencia,
- Asegura a tus clientes y socios que tu empresa se adelanta a los nuevos requisitos
- Te sitúa a la vanguardia del cumplimiento normativo

Ponte en contacto con nosotros para obtener más información sobre cómo la marca Applus+ Cyber Resilience puede elevar el posicionamiento de tu empresa en el ámbito de la ciberseguridad y proporcionar una ventaja competitiva en el mundo digital actual.