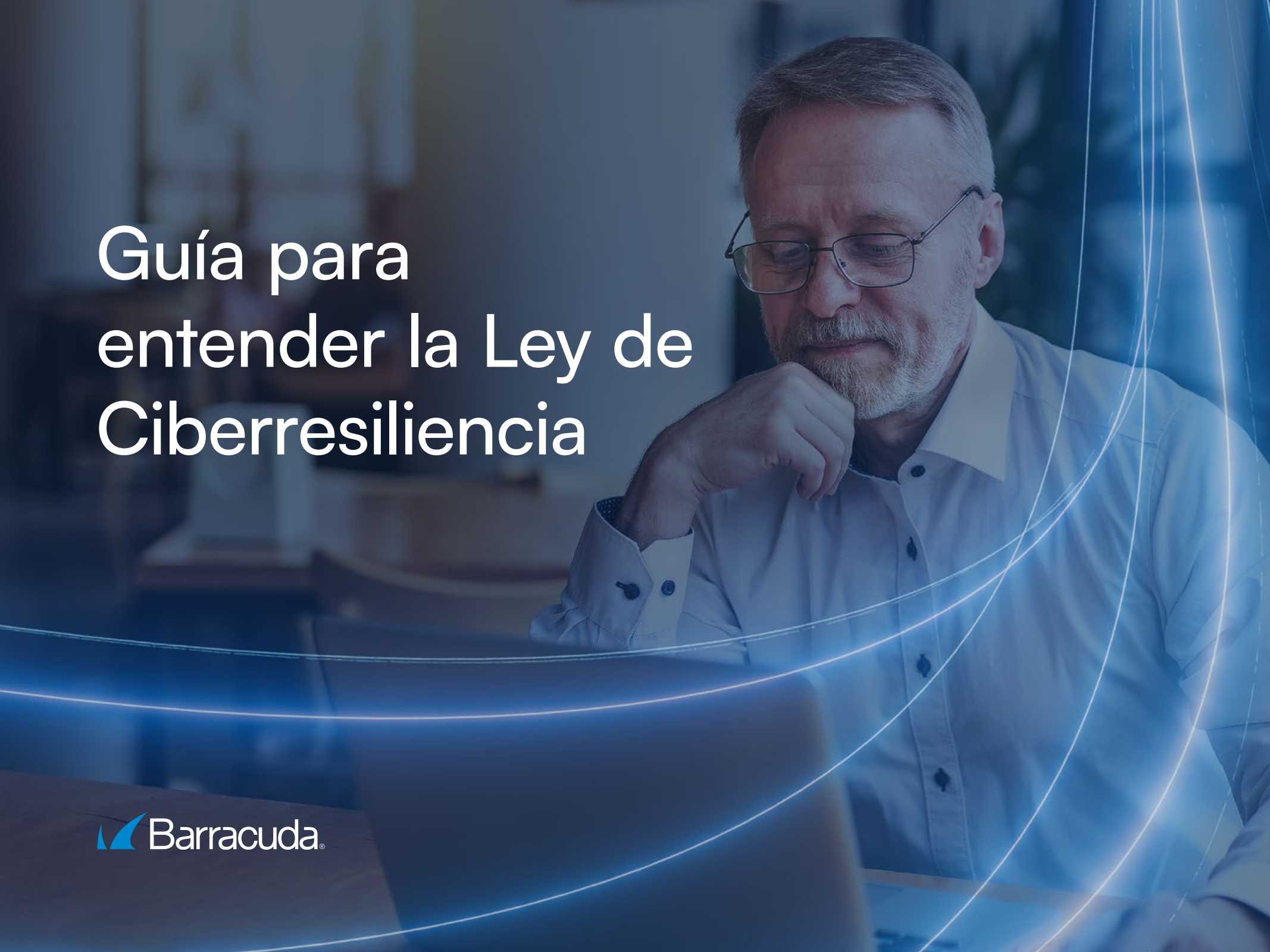

Guía para entender la Ley de Ciberresiliencia

Barracuda

Comprender la Ley de Ciberresiliencia (CRA) de la Unión Europea (UE) es esencial para las organizaciones que operan en la UE. Los fabricantes de productos digitales que se comercializan en la UE, así como los importadores y distribuidores de dichos productos, están sujetos a la CRA. Este e-book ofrece algunos aspectos destacados de la CRA para fabricantes, pero no sustituye ni pretende servir de asesoramiento jurídico para su empresa.

La CRA entró en vigor en diciembre de 2024, lo que dio a las organizaciones un plazo para lograr el cumplimiento normativo. Estas son algunas fechas clave que conviene conocer:

- 11 de septiembre de 2026: Los fabricantes deben empezar a notificar los incidentes graves de ciberseguridad y las vulnerabilidades explotadas activamente.
- 11 de diciembre de 2027: Todos los productos nuevos y cualquier producto existente «sustancialmente modificado» que se comercialice a partir de esta fecha deben cumplir la CRA.

La ley pretende ofrecer un conjunto más uniforme de requisitos de seguridad para todos los productos con elementos digitales que se vendan en la UE y proporcionar a los consumidores y empresas que adquieran estos productos más información sobre su seguridad antes de comprarlos. La ley aspira a rectificar lo que la UE describe como el «nivel inadecuado» de ciberseguridad presente en muchos productos, incluida la falta de actualizaciones de seguridad.

La CRA complementa la Ley de Resiliencia Operativa Digital (DORA) y la Directiva sobre Seguridad de las Redes y de la Información 2 (NIS2):

- DORA se centra en mejorar la ciberresiliencia del sector financiero, mientras que NIS2 se aplica a un conjunto más amplio de entidades que prestan servicios esenciales en sectores clave.
- Tanto DORA como NIS2 especifican requisitos de ciberseguridad, incluidas medidas de seguridad de la cadena de suministro, con el fin de aumentar la resiliencia de las empresas reguladas, dado el impacto que tienen sus productos y servicios en terceros.
- La CRA se aplica a nivel de producto y establece el marco obligatorio para productos seguros con elementos digitales. Cuando el cliente de dichos productos está regulado por DORA o NIS2, el uso de hardware y software conformes con la CRA puede ayudar a estas entidades a cumplir sus obligaciones.

NIS2 y DORA quedan fuera del alcance de este libro electrónico. Consulte Comprender DORA: una guía para la Ley de Resiliencia Operativa Digital y Recorrido por la NIS2: guía de las próximas normativas europeas sobre ciberseguridad para obtener más información.

¿Por qué es importante la CRA?

La CRA abarca todos los productos que contengan «elementos digitales», lo que significa que este reglamento cubre tanto el hardware como el software conectado a un dispositivo o red, además de las soluciones integradas de procesamiento remoto de datos de dichos productos (es decir, los servicios en la nube). Según la Comisión Europea, «el reglamento se aplica a todos los productos conectados directa o indirectamente a otro dispositivo o red, salvo exclusiones específicas como determinados productos de software o servicios de código abierto que ya están cubiertos por normas vigentes, como es el caso de los productos sanitarios, la aviación y los automóviles».[1] No se permitirá la venta en la UE de los productos que no cumplan la normativa. Las organizaciones que lo hagan se enfrentarán a multas. Del mismo modo que el Reglamento General de Protección de Datos (RGPD) cambió radicalmente la forma en que las empresas gestionan la información personal, la CRA tiene el potencial de producir un efecto similar en la manera en que los fabricantes producen, venden y dan soporte a sus productos con elementos digitales comercializados en la UE.

La CRA aborda un problema creciente con los productos tecnológicos modernos que recopilan, tratan, comparten y almacenan datos de los usuarios —a menudo sin seguridad o con una seguridad débil—, lo que pone en riesgo dichos datos. A medida que estos productos maduran, las soluciones de seguridad disponibles pueden quedar obsoletas. Existe poca supervisión sobre cómo, cuándo o si se proporcionan actualizaciones de seguridad a los usuarios. La CRA pretende aumentar la seguridad de los productos con elementos digitales y garantizar que dichos productos sigan siendo seguros durante todo su ciclo de vida. La ley también proporcionará una mayor transparencia a los usuarios, que comprenderán mejor la seguridad de los productos con elementos digitales y cómo podría afectar a sus datos.

[1] Cyberresilienz-Verordnung | Gestaltung der digitalen Zukunft Europas

Obligaciones de la CRA para los fabricantes

La CRA introduce requisitos obligatorios de ciberseguridad para los fabricantes que regulan la planificación, el diseño, el desarrollo, la producción, la entrega, la documentación y el mantenimiento de dichos productos. Estas obligaciones deben cumplirse en todas las etapas de la cadena de valor.

En virtud de la CRA, los productos pueden clasificarse como estándar (nivel más bajo), «importantes» (con más obligaciones) —que se dividen en dos subcategorías: importante de clase I e importante de clase II— y «críticos» (con el mayor nivel de riesgo y, por tanto, de obligaciones).

En el caso de los artículos estándar, los fabricantes deben diseñar, fabricar y probar los productos y servicios para garantizar el cumplimiento normativo de los «requisitos esenciales de seguridad» especificados en el Anexo I de la CRA, documentar la evaluación y mantener la documentación técnica a disposición de las autoridades de vigilancia del mercado. En este nivel, los fabricantes pueden basarse en una evaluación de conformidad interna (autoevaluación).

En términos generales, se espera que alrededor del 90 % de los productos de hardware y software entren en esta categoría estándar, lo que permite a los fabricantes autoevaluarse y elaborar una declaración de conformidad antes de aplicar el marcado CE que recibirán los productos conformes.

Ciertos productos con elementos digitales —como navegadores web, firewalls y sistemas operativos— entran en la categoría «importantes», y otros incluso en la categoría «críticos». Estos deben seguir cumpliendo los requisitos técnicos del Anexo I, pero pueden estar sujetos a un proceso de evaluación de la conformidad más estricto, que incluya la evaluación/certificación por parte de terceros antes de su venta en la UE.

Además de las obligaciones en el momento de la venta, la CRA también exige a los fabricantes que proporcionen gestión de vulnerabilidades y parches de seguridad, tal y como se describe a continuación.

Obligaciones de notificación de seguridad

La notificación de vulnerabilidades de seguridad aprovechadas activamente y de incidentes graves en virtud de la CRA entrará en vigor el 11 de septiembre de 2026.

Las obligaciones de notificación son estrictas. Los fabricantes deberán enviar una notificación de «alerta temprana» a los reguladores en un plazo de 24 horas desde que tengan conocimiento del problema. En un plazo de 72 horas desde que tengan conocimiento de una vulnerabilidad aprovechada, los fabricantes deberán proporcionar información general sobre el producto afectado, una descripción general de la vulnerabilidad aprovechada y cualquier medida de mitigación que haya tomado el fabricante y que los usuarios puedan tomar, así como indicar la sensibilidad del problema. Dentro de los 14 días siguientes a la disponibilidad de las medidas de mitigación, el fabricante tiene obligaciones de divulgación adicionales, en el sentido de un informe final.

Las obligaciones de notificación también incluyen informar a los usuarios afectados y asesorarles sobre las formas de mitigar la exposición.

Los fabricantes deben familiarizarse con estos requisitos de notificación y desarrollar procesos para cumplirlos antes de la fecha de inicio de septiembre de 2026.

Barracuda

Obligaciones de soporte técnico

El soporte de ciberseguridad, en el sentido de proporcionar actualizaciones de seguridad, también es un tema importante en la CRA y debe planificarse para cubrir todo el ciclo de vida del producto. Los fabricantes deben especificar por adelantado el periodo de soporte para los productos con elementos digitales. En general, las empresas que comercialicen productos con elementos digitales en la UE deben prestarles soporte durante al menos cinco años, salvo que la vida útil prevista del producto sea inferior a cinco años; en ese caso, el soporte debe durar lo que dure la vida útil prevista del producto. En el caso de los productos que suelen tener una vida útil superior a cinco años (por ejemplo, placas base, routers de red, módems, conmutadores y sistemas operativos), el periodo de soporte debe ser más largo. Las actualizaciones de seguridad disponibles durante el período de soporte deben estar a disposición de los usuarios durante el período de soporte más largo o durante 10 años, lo que sea más largo.

¿Cómo se hará cumplir la normativa?

El incumplimiento puede dar lugar a sanciones, tanto económicas —multas de hasta 15 millones de euros o el 2,5 % de la facturación global total— como no económicas. Los reguladores podrían obligar a una empresa a retirar los productos que no cumplan la normativa.

Barracuda

Seis pasos hacia el cumplimiento normativo para los fabricantes

A continuación se indican los pasos básicos que deben seguir los fabricantes para iniciar su proceso de cumplimiento normativo y estar preparados cuando la CRA entre plenamente en vigor. Los múltiples anexos de la CRA proporcionan detalles sobre lo que se espera en cada paso.

1. Clasificar los productos y efectuar una evaluación de riesgos cibernéticos. Las organizaciones pueden tener productos en múltiples categorías. Por lo tanto, es importante evaluar cada producto para determinar en qué categoría se incluye: estándar, importante o crítico.

2. Preparar la documentación técnica. Revisar el Anexo I de la CRA y los requisitos de la cadena de suministro para todos los productos e identificar cualquier deficiencia. Efectuar y documentar una evaluación de riesgos para cada producto en función de los criterios aplicables y las normas, especificaciones comunes o sistemas de certificación adecuados identificados.

3. Determinar el enfoque de evaluación de la conformidad de cada producto. Si es necesario, contratar a un tercero para esta tarea.

4. Preparar una declaración de conformidad conforme a los anexos V/VI y completar la documentación técnica que cubra el contenido del anexo VII. A continuación, el fabricante debe aplicar el marcado CE a un producto conforme, a su embalaje o a su documentación. El marcado CE indicará la conformidad de los productos con elementos digitales con la CRA, de modo que puedan circular libremente dentro de la UE.

Barracuda

5. Preparar y proporcionar información e instrucciones para el usuario según el Anexo II. La documentación es una parte fundamental del cumplimiento normativo y su objetivo es proporcionar transparencia al usuario.

6. Supervisar y gestionar las vulnerabilidades. La CRA exige la participación activa y continua de los fabricantes durante el periodo de cobertura del soporte, lo que incluye prestar soporte de ciberseguridad, supervisar cualquier vulnerabilidad, y notificar y corregir los problemas detectados, por ejemplo mediante actualizaciones de software que aborden cuestiones de seguridad.

Barracuda está trabajando activamente para confirmar sus categorías de productos y abordar los siguientes pasos. Proporcionaremos información sobre el Trust Center cuando esté disponible.

PASO 1
Clasificar los productos y efectuar una evaluación de riesgos cibernéticos Evaluación para cada uno

PASO 2
Preparar la documentación técnica

PASO 3
Determinar el enfoque de evaluación de la conformidad

PASO 4
Aplicar el marcado CE y redactar la declaración de conformidad

PASO 5
Preparar y proporcionar instrucciones para el usuario

PASO 6
Supervisar y gestionar las vulnerabilidades

Importante de clase I e importante de clase II

Los productos importantes de clase I suponen un riesgo de ciberseguridad menor que los productos importantes de clase II. Los fabricantes pueden optar por autodeclarar el cumplimiento si cumplen determinadas normas, especificaciones comunes o sistemas de certificación cualificados de la UE, siempre que estén disponibles y sean aplicables al producto. De lo contrario, es posible que se requiera una verificación por parte de un tercero.

Se considera que los productos importantes de clase II presentan un mayor nivel de riesgo para la ciberseguridad, por lo que se requiere la certificación de un tercero autorizado.

La CRA, DORA y NIS2 conforman conjuntamente un complejo conjunto de normativas de ciberseguridad para las empresas que operan en la UE. Es posible que su empresa esté sujeta a más de una de estas normativas. El Trust Center de Barracuda contiene múltiples recursos para ayudar a los clientes a comprender DORA, incluido nuestro e-book Comprender DORA: una guía para la Ley de Resiliencia Operativa Digital y NIS2, incluido nuestro e-book Recorrido por NIS2: guía de las próximas normativas europeas sobre ciberseguridad, para ayudar a las empresas con sus obligaciones de cumplimiento normativo.

Sobre Barracuda

Barracuda es una empresa líder mundial en ciberseguridad que ofrece protección completa frente a amenazas complejas para empresas de todos los tamaños. Su plataforma BarracudaONE, basada en IA, protege el correo electrónico, los datos, las aplicaciones y las redes con soluciones innovadoras, XDR gestionado y un panel centralizado para maximizar la protección y reforzar la ciberresiliencia. Con la confianza de cientos de miles de profesionales de TI y proveedores de servicios gestionados en todo el mundo, Barracuda ofrece defensas potentes que son fáciles de adquirir, implementar y utilizar. Para obtener más información, visite es.barracuda.com.

Barracuda®