

# Cumpla con la NIS 2 con total confianza

Acronis

La directiva NIS 2 es crucial para las organizaciones, ya que exige la adopción de medidas de ciberseguridad más estrictas y una mayor responsabilidad a la hora de proteger servicios esenciales en la UE.

Sin embargo, comprender e implementar las medidas que exige la directiva NIS 2 puede ser muy complicado debido a su complejidad, a sus estrictos requisitos y al lenguaje en el que se redactó, que suele ser ambiguo. Esto hace difícil desglosar la directiva en pasos claros y factibles, lo que deja

a muchas organizaciones sin saber por dónde empezar o cómo garantizar el pleno cumplimiento normativo.

Este documento sirve de guía para simplificar la directiva NIS 2 mediante el desglose de sus requisitos y asigna a cada uno de ellos el producto de Acronis más recomendado para cumplirlos. Además, proporciona a las organizaciones pasos claros y factibles para ayudarlas a cumplir con las normativas y a ceñirse a la directiva con total confianza.

## Acronis puede ayudar a cumplir con muchas medidas de la directiva NIS 2

Medidas de la NIS 2	Funciones de Acronis	Cómo ayuda Acronis
<b>Gestión de riesgos y administración</b> Identificar, abordar y supervisar los riesgos de ciberseguridad para garantizar una protección eficaz y el cumplimiento de las normativas. <b>Artículo 20</b> (Requisitos de administración) <b>Artículo 21</b> (Medidas de gestión del riesgo)	<b>Administración de endpoints</b> (Incluido en Acronis Cyber Protect <b>Advanced</b> )	Herramientas de inventario exhaustivas que descubren, rastrean y generan informes de todos los recursos de hardware y software.
	<b>Administración de endpoints: evaluación de vulnerabilidades</b> (Incluido en Acronis Cyber Protect <b>Standard, Advanced y Backup Advanced</b> )	Permite descubrir cualquier vulnerabilidad antes de que alguien la aproveche.
<b>Gestión de incidentes y generación de informes</b> Detectar los incidentes de ciberseguridad de forma eficaz e informar de ellos a las partes interesadas. <b>Artículo 10</b> (Equipos de respuesta ante incidentes de seguridad informática) <b>Artículo 23</b> (Obligaciones de generación de informes)	<b>Detección y respuesta para endpoints (EDR)</b> (Incluido en Acronis Cyber Protect <b>Advanced</b> )	Recopila telemetría relevante para la seguridad de los endpoints, así como registros del sistema para detectar anomalías e impulsar una respuesta informada en todos los endpoints afectados. Integración con fuentes de información sobre amenazas. Respuesta y corrección automatizadas.
	<b>Funciones esenciales de administración de la seguridad y antimalware</b> (Incluido en Acronis Cyber Protect <b>Standard y Advanced</b> )	Administración de parches con aplicación de parches a prueba de fallos: se realizan copias de seguridad de los endpoints antes de instalar los parches. Crea listas de URL admitidas y no admitidas, y analiza la carga útil de las URL maliciosas.
	<b>Funciones avanzadas de administración de la seguridad y antimalware</b> (Incluido en Acronis Cyber Protect <b>Advanced</b> )	Bloquea el malware antes de que afecte a los datos. Protección en tiempo real con heurística estática y de comportamientos basadas en IA, antivirus, antimalware, antiransomware y anticryptojacking.
	<b>Ciberseguridad: Centros de operaciones de ciberprotección (CPOC)</b>	Supervisan continuamente el panorama de la ciberseguridad y envían alertas en tiempo real sobre posibles amenazas, como malware, vulnerabilidades, desastres naturales y otros acontecimientos mundiales.

Medidas de la NIS 2	Funciones de Acronis	Cómo ayuda Acronis
<p><b>Continuidad de la actividad empresarial</b> Mantener las operaciones esenciales y recuperarse rápidamente de posibles interrupciones o incidentes de ciberseguridad.</p> <p><b>Artículo 21</b> (Medidas de gestión del riesgo)</p>	<p><b>Funciones de copia de seguridad básicas</b> (Incluido en Acronis Cyber Protect <b>Standard, Advanced y Backup Advanced</b>)</p>	<p>Copia de seguridad: recuperación en hardware diferente desde cero, basada en archivos o en imágenes.</p> <p>Protección de datos para servidores físicos y virtuales, aplicaciones y bases de datos, estaciones de trabajo, Microsoft 365 y Google Workspace.</p> <p>Almacenamiento inmutable en la nube.</p>
	<p><b>Recuperación ante desastres</b> (Complemento: Acronis Cyber Protect <b>Standard, Advanced o Backup Advanced</b>)</p>	<p>La función One-Click Recovery permite a cualquier usuario recuperar un endpoint que ha fallado sin necesidad de que el equipo de TI intervenga.</p> <p>Con la recuperación ante desastres, es posible reanudar rápidamente las operaciones empresariales tras una falla generalizada.</p> <p>Pruebas de recuperación ante desastres (DR), conmutación por error y conmutación tras recuperación automatizadas para recursos informáticos físicos y virtuales.</p>
	<p><b>Funciones avanzadas de administración de la seguridad y antimalware</b> (Incluido en Acronis Cyber Protect <b>Advanced</b>)</p>	<p>Recuperación segura con análisis y corrección de copias de seguridad previas a la restauración para detectar malware y vulnerabilidades.</p>

Los productos y servicios de Acronis son herramientas esenciales para las empresas y organizaciones que deben cumplir con la directiva NIS 2, ya que permiten abordar áreas clave como la ciberseguridad y la gestión de incidentes. Sin embargo, el cumplimiento real también exige procesos sólidos, una administración eficaz y una supervisión proactiva.

## Descubra cómo Acronis puede ayudarle a cumplir con la directiva

**OBTENER MÁS INFORMACIÓN**

