

¿Se aplica NIS2 a su empresa?

Tres comprobaciones basadas en la Ordenanza de Urgencia rumana (OUG) 155/2024, en su versión consolidada aplicable. La aplicabilidad depende del tipo de entidad y la actividad del anexo, no solo del nombre general del sector.

1 ¿Opera en uno de los 18 sectores?

ANEXO 1 · SECTORES DE ALTA CRITICIDAD

- ☐ **Energía** (electricidad, calefacción y refrigeración urbanas, petróleo, gas, hidrógeno)
- ☐ **Transporte** (aéreo, ferroviario, acuático; por carretera: autoridades viarias y operadores de sistemas inteligentes de transporte)
- ☐ **Banca** (véase la nota DORA)
- ☐ **Infraestructuras de los mercados financieros** (véase DORA)
- ☐ **Salud** (asistencia sanitaria, producción y distribución farmacéuticas, farmacias)
- ☐ **Agua potable**
- ☐ **Aguas residuales**
- ☐ **Infraestructura digital** (DNS, TLD, nube, centros de datos, comunicaciones electrónicas, servicios de confianza)
- ☐ **Servicios TIC gestionados** (incluidos los servicios de seguridad gestionados)
- ☐ **Administración pública central**
- ☐ **Espacio**

ANEXO 2 · OTROS SECTORES CRÍTICOS

- ☐ **Servicios postales y de mensajería**
- ☐ **Gestión de residuos** (si es la actividad principal)
- ☐ **Productos químicos** (fabricación, producción, distribución)
- ☐ **Alimentación** (producción y transformación industriales, distribución mayorista)
- ☐ **Fabricación** (productos sanitarios, electrónica y óptica, equipos eléctricos, maquinaria, vehículos y otros equipos de transporte)
- ☐ **Proveedores digitales** (mercados en línea, motores de búsqueda, redes sociales)
- ☐ **Investigación**

Base: anexos 1 y 2 de la OUG 155/2024

Transporte por carretera: otras actividades o circunstancias pueden motivar la inclusión. **DORA:** las entidades financieras sujetas a DORA evalúan el riesgo TIC bajo el régimen sectorial especial. Figurar en un anexo NIS2 no implica acumular íntegramente las mismas obligaciones. La identificación y el registro se comprueban por separado.

2 ¿Cumple los criterios legales de tamaño?

La plantilla no es el único criterio. Menos de 50 empleados no implica una exclusión automática. Compruebe los umbrales legales, las empresas asociadas o vinculadas y las categorías sujetas con independencia del tamaño.

- ☐ **Mediana:** 50–249 empleados y facturación ≤ 50 millones EUR o activos ≤ 43 millones EUR.
- ☐ **Grande:** supera los umbrales de la mediana empresa.
- ☐ **Sujetas con independencia del tamaño:** por ejemplo, administración pública central, servicios DNS, registros TLD y servicios de confianza. Lista no exhaustiva.

Base: arts. 5–9, OUG 155/2024; art. 4, Ley 346/2004

3 ¿Tiene clientes en estos sectores?

- ☐ **Suministramos productos o servicios a entidades de los sectores en la etapa 1** (IT, software, mantenimiento, logística, consultoría, o cualquier servicio con acceso a sus sistemas o datos)

Las entidades sujetas deben gestionar los riesgos de seguridad de proveedores directos y prestadores, y pueden exigir condiciones contractuales proporcionales al riesgo (arts. 11 y 13, OUG 155/2024).

CÓMO INTERPRETAR EL RESULTADO

Sector del anexo 1 y gran empresa; administración pública central, servicios DNS, registros TLD, servicios de confianza cualificados

Muy probablemente una entidad esencial
Art. 5

Sector del anexo 1 y mediana empresa; sector del anexo 2 y mediana o gran empresa

Muy probablemente una entidad importante
Existen excepciones: algunas categorías son esenciales aun siendo medianas o con independencia del tamaño, incluidos los proveedores de seguridad gestionada (MSSP). La clasificación final se verifica según los arts. 5–9 de la OUG 155/2024.

Sólo se aplica el paso 3

Aunque no cumpla por sí mismo los criterios de aplicabilidad directa, los clientes sujetos pueden exigir medidas contractuales de seguridad. Ser proveedor no determina por sí solo la aplicabilidad de NIS2.

Calendario de obligaciones

Los plazos parten de acontecimientos distintos para cada entidad. Determine primero en qué punto del proceso se encuentra.

PLAZO	OBLIGACIÓN	INICIO DEL PLAZO Y REQUISITOS	BASE
30 días	Notificación para el registro	Presentar dentro de los 30 días siguientes a la fecha en que la entidad esté sujeta a las disposiciones aplicables.	Art. 18(2)
30 días	Designación del responsable de seguridad	De la notificación de la decisión de registro, con sujeción a las condiciones para el papel y la categoría de entidad. Un contrato de apoyo a la TI no constituye, por sí mismo, el nombramiento legal.	Art. 14(3)–(4)
60 días	Envío de la evaluación del nivel de riesgo	Para las entidades sujetas a este procedimiento: desde la notificación de la decisión de registro, el nivel de garantía resultante difiere de la condición jurídica de entidad importante o esencial.	Art. 18(6)
60 días	Autoevaluación inicial de madurez	Preparar y presentar dentro del plazo reglamentario de 60 días a partir de la presentación de la evaluación del nivel de riesgo.	Art. 18(7)
30 días	Envío del plan de medidas correctoras	Las entidades esenciales presentan el plan dentro de los 30 días siguientes a la autoevaluación. Este es el plazo para presentar el plan, no para completar toda la remediación.	Art. 12(5)
Anualmente	Autoevaluación periódica	Realizado anualmente, refrendado por la administración y presentado con arreglo al procedimiento aplicable.	Art. 12(4)
24 h · 72 h	Notificación de un incidente significativo	Alerta temprana en 24 horas y notificación en 72 horas desde que se conoce el incidente. Informe final en un mes desde la notificación, con reglas especiales para incidentes en curso. Informe intermedio a petición de la autoridad; plazo especial para prestadores de servicios de confianza.	Art. 15(7)–(8)

MÁS ALLÁ DE LOS TRÁMITES

Las medidas van más allá del registro

El registro y la autoevaluación no sustituyen la aplicación: gestión de riesgos, seguridad de accesos y sistemas, gestión de incidentes, continuidad, copias de seguridad, seguridad de proveedores, formación y verificación de eficacia.

Base: arts. 11 y 13, OUG 155/2024

PARA LA REUNIÓN DE DIRECCIÓN

Cinco preguntas que plantear

☐ ¿Sabemos, por escrito, si somos una entidad esencial, una entidad importante o sólo un proveedor?

☐ ¿Hemos presentado la notificación de registro y recibido la decisión de registro?

☐ ¿Quién es responsable de la seguridad, y a quién reportan?

☐ ¿Podemos probar que hacemos lo que nuestras políticas dicen?

☐ ¿Alguien sabe qué hacer en las primeras 24 horas después de un incidente?

ART. 60 DE OUG 155/2024

Qué establece la ley

- Violaciones administrativas:** ciertos incumplimientos, incluido el incumplimiento de las obligaciones de registro, atraen las penas por los actos enumerados en el artículo 60. El límite depende de la categoría de incumplimiento y entidad.
- Límite máximo:** para las infracciones sujetas a estos límites, el mayor entre el importe fijo y el porcentaje legal del volumen de negocios anual mundial total del ejercicio anterior: 7 millones EUR o 1,4 % para entidades importantes; 10 millones EUR o 2 % para entidades esenciales. La multa se fija conforme a la ley.
- La dirección** aprueba y supervisa las medidas y tiene obligaciones de formación. Responde, en las condiciones legales, por el incumplimiento de sus deberes (art. 14).

RECUERDE

La autoevaluación abarca la documentación y la aplicación efectiva. Para determinados proveedores digitales y servicios gestionados, compruebe también el Reglamento de Ejecución (UE) 2024/2690.

¿Necesita una evaluación de aplicabilidad razonada?

Clarified IT prepara su ficha de aplicabilidad con una conclusión fundamentada, obligaciones y un calendario preliminar.

it.clarified.ro/nis2
office@clarified.ro · +40 774 456 127

Fuentes: OUG 155/2024, aprobada con enmiendas y adiciones por la Ley 124/2025, en su forma consolidada aplicable; Directiva 2022/2555; Reglamento (UE) 2022/2554 (DORA); Ley 346/2004. Esta lista de verificación es informativo: ofrece orientación basada en la información disponible y no reemplaza la evaluación de la situación específica o la decisión o poderes de la autoridad.