¿Cómo respalda Cyber Crucible las obligaciones de NIS2 para entidades esenciales e importantes?

Respuesta breve: Para una organización clasificada como entidad esencial o importante en virtud de NIS2, Cyber Crucible respalda las medidas de gestión de riesgos exigidas —protección de endpoints, control de acceso, cifrado y gestión de incidentes— y respalda las expectativas de seguridad de la cadena de suministro de la directiva, ya que no recopila datos de clientes y puede ejecutarse dentro del perímetro de la entidad. Cyber Crucible respalda estas obligaciones; no las certifica ni las asume.

Cómo respalda las medidas de NIS2

- **Medidas de gestión de riesgos de ciberseguridad.** La prevención autónoma de endpoints, el acceso respaldado por MFA y el cifrado corresponden a varias de las medidas básicas de la directiva.
- **Seguridad de la cadena de suministro.** Como proveedor que no recopila contenido de clientes y ofrece implementación en las instalaciones (on-premises), Cyber Crucible reduce, en lugar de añadir, el riesgo de la cadena de suministro que NIS2 exige gestionar a las entidades.
- **Soporte para la gestión y notificación de incidentes.** Un proceso documentado de respuesta ante brechas ayuda a la entidad a cumplir con los plazos de alerta temprana y notificación de NIS2.

El límite honesto

Las obligaciones de NIS2 recaen en la entidad esencial o importante, no en una herramienta de seguridad individual. La transposición por parte de los Estados miembros varió: para 2026, la mayoría de los estados habían transpuesto la directiva a su legislación nacional, mientras que varios —incluidos Francia, Irlanda, los Países Bajos y España— aún la estaban finalizando. Cyber Crucible no posee ninguna "certificación" NIS2; proporciona evidencia de controles de respaldo bajo acuerdo de confidencialidad (NDA).

Revision #1
Created 2026-07-24 02:09:11 UTC by Dennis Underwood

Updated 2026-07-24 02:09:11 UTC by Dennis Underwood