ManageEngine

# Doble problema o doble defensa: qué significan NIS2 y DORA para las finanzas

# La resiliencia es el nuevo estándar de cumplimiento

En finanzas, el riesgo es un lenguaje que usted domina a la perfección. Pero hoy en día, el riesgo no es solo la volatilidad del mercado, sino también los ciberataques, las interrupciones del servicio en la nube y los fallos en la cadena de suministro, que golpean más rápido que una caída repentina. Para controlar esta fragilidad digital, la Unión Europea (UE) ha introducido dos mandatos de cumplimiento de gran peso:

Directiva sobre redes y sistemas de información (NIS2): Centrada en impulsar la ciberseguridad en sectores clave, incluido el financiero.

Ley de Resiliencia Operativa Digital (DORA): Su objetivo es hacer que las instituciones financieras sean más resistentes a las interrupciones de TI.

No se trata de normas duplicadas, sino de las dos caras de la misma moneda. Y, como organización financiera, se espera que cumpla con ambas. Por lo tanto, la verdadera pregunta no es por qué debe cumplir, sino ¿con qué rapidez puede adaptarse?

# El desglose inteligente: NIS2 frente a DORA para entidades financieras

| Categoría | Directiva NIS2 | Ley DORA |
|---|---|---|
| Naturaleza | Directiva: requiere transposición nacional. | Ley: directamente aplicable en toda la UE. |
| Se aplica a | Todos los sectores esenciales (energía, salud, finanzas, etc.) | Solo entidades financieras y sus proveedores de TIC. |
| Objetivo principal | Elevar los estándares básicos de ciberseguridad en todos los sectores. | Garantizar que las organizaciones financieras puedan sobrevivir y recuperarse de las interrupciones de las TIC. |
| Enfoque en el riesgo | Cyber protection, incident handling, and supply chain security | Resiliencia de las TIC, continuidad, pruebas de recuperación y supervisión de proveedores. |
| Responsabilidad de la junta directiva | Gobernanza y rendición de cuentas obligatorias a nivel de liderazgo | Igual que NIS2: supervisión explícita de la junta directiva para la resiliencia y la preparación ante incidentes. |
| Escrutinio de terceros | Supervisión prevista de los proveedores de servicios | Supervisión exhaustiva: escrutinio crucial de los proveedores de TIC y obligaciones contractuales de resiliencia. |
| Plazos para presentar informes | Notificar los incidentes en un plazo de 24 horas. | Informes estructurados sobre incidentes y recuperaciones de TIC dentro de plazos estrictos. |
| Sanciones | Hasta 10 millones de euros o el 2 % de la facturación global. | No establece multas fijas, pero los proveedores de TIC pueden enfrentarse a sanciones diarias del 1 % de su facturación global media durante un máximo de seis meses hasta que cumplan con la normativa. |

# Mitos comunes sobre NIS2 y DORA

**Mito 1:**

## Si tanto la NIS2 como la DORA se aplican a usted, basta con cumplir únicamente con la DORA

Aunque la DORA tiene prioridad como normativa específica del sector, no sustituye a la NIS2. Las instituciones financieras deben seguir cumpliendo los requisitos generales de la NIS2, como la cooperación intersectorial y el intercambio de información, ámbitos en los que la DORA no ofrece una cobertura completa. El cumplimiento total implica ajustarse a ambos marcos, no solo a uno.

Por ejemplo, supongamos que un banco sufre un ciberataque que interrumpe sus sistemas de comunicación interna. Sigue el proceso de notificación de incidentes de la DORA y envía un informe al regulador financiero. Sin embargo, la NIS2 exige la notificación a las autoridades nacionales de ciberseguridad y también puede exigir la coordinación con los equipos de respuesta a incidentes de seguridad informática y las autoridades sectoriales, dependiendo de la naturaleza de la interrupción. Si el banco solo notifica el incidente en virtud de la DORA y no recurre a los mecanismos de la NIS2, corre el riesgo de incurrir en un incumplimiento parcial.

**Mito 2:**

## Si cuento con la certificación ISO 27001, cumplo automáticamente con NIS2 y DORA

Si bien la norma ISO 27001 puede proporcionar una base sólida, no sustituye al cumplimiento de la NIS2 o la DORA. Ambos marcos tienen requisitos legales específicos, como obligaciones de notificación, cooperación en materia de supervisión y clasificación de riesgos, que las normas ISO no cubren.

Por ejemplo, una organización puede tener controles y políticas bien documentados y alineados con la norma ISO 27001, pero aún así carecer de un mecanismo para clasificar los incidentes relacionados con las TIC según los niveles de gravedad de la DORA o no cumplir con el plazo inicial de notificación de 24 horas exigido por la NIS2. Del mismo modo, la norma ISO 27001 no exige la colaboración con organismos de supervisión nacionales o de la UE ni la realización de ejercicios de simulación de amenazas específicos para cada sector. Los reguladores pueden considerar esto como una laguna, lo que pone de relieve que la norma ISO ayuda, pero no cumple todos los requisitos.

**Mito 3:**

## La externalización de los servicios de TI o ciberseguridad transfiere la responsabilidad del cumplimiento de las normas NIS2 y DORA al proveedor de servicios.

Aunque externalice los servicios de TI, la infraestructura en la nube o las operaciones de ciberseguridad, su organización sigue siendo plenamente responsable del cumplimiento tanto de la NIS2 como de la DORA. Estas normativas dejan claro que la entidad obligada conserva la responsabilidad legal y operativa de la gestión de riesgos, la notificación de incidentes, la gobernanza y la supervisión de terceros.

Por ejemplo, según la DORA, debe evaluar y supervisar a sus proveedores externos de TIC, garantizar el cumplimiento contractual e informar sobre su postura en materia de resiliencia. Del mismo modo, la NIS2 espera que comprenda y controle los riesgos en toda su cadena de suministro. La delegación no es una exención. Si algo sale mal, los reguladores acudirán a usted, no a su proveedor.

# Adopte un enfoque unificado para el doble cumplimiento con ManageEngine

ManageEngine ayuda a las organizaciones a cumplir con las normativas NIS2 y DORA mediante el refuerzo de su gobernanza general de TI, su postura de ciberseguridad y su resiliencia operativa.

## Cómo le ayudan las soluciones de ManageEngine a cumplir con la normativa

| Para el cumplimiento de la norma NIS2 | Para el cumplimiento de la DORA |
|---|---|
| Implementa controles de acceso estrictos y segmentación de red para proteger los sistemas críticos. | Aplica el acceso basado en privilegios y la segregación de funciones para controlar los riesgos internos relacionados con las TIC. |
| Detecta amenazas en tiempo real y gestiona vulnerabilidades en terminales e infraestructura. | Integra el riesgo de las TIC en la gestión de riesgos empresariales y evalúa continuamente los riesgos digitales. |
| Mantiene registros de auditoría detallados y apoya la detección y notificación de incidentes dentro de los plazos establecidos. | Garantiza el análisis del impacto de los incidentes, los plazos de presentación de informes y la documentación de las causas fundamentales. |
| Permite la supervisión continua y la visibilidad centralizada de los sistemas de red y de información. | Permite estrategias avanzadas de resiliencia operativa, incluyendo pruebas de estrés y simulaciones. |
| Apoya las políticas de gobernanza y la rendición de cuentas en todos los sistemas de tecnología de la información y tecnología operativa. | Realiza un seguimiento del cumplimiento de los marcos de riesgo y apoya la supervisión de la resiliencia digital por parte del consejo de administración. |
| Ayuda en la coordinación de la respuesta a amenazas específicas del sector y en la presentación de informes reglamentarios. | Garantiza la supervisión de los proveedores externos de TIC y gestiona los riesgos de la externalización. |

Descubra cómo ManageEngine simplifica ambos procesos:
mnge.it/es/nis2 | mnge.it/es/dora

Además, las soluciones de ManageEngine admiten pruebas periódicas de la infraestructura digital y proporcionan herramientas para mantener la documentación de cumplimiento y la trazabilidad en todos los entornos de TI. Al permitir la visibilidad, el control y la automatización en diversas operaciones de TI, ManageEngine ayuda a las empresas a cumplir tanto con las exigencias de ciberseguridad de la NIS2 como con los requisitos de resiliencia y gestión de riesgos de la DORA, lo que les permite reducir el riesgo normativo y garantizar la prestación ininterrumpida de servicios digitales.

Descargo de responsabilidad: La implementación completa de DORA y NIS2 requiere una variedad de procesos, políticas, personal y controles tecnológicos. Junto con otras soluciones, procesos, controles de personal y políticas adecuadas, las soluciones de ManageEngine pueden ayudar a las organizaciones a alinearse con DORA y NIS2. Las organizaciones deben realizar una evaluación independiente de las características de ManageEngine e identificar en qué medida pueden ayudarles a cumplir con estas directivas. Este material se proporciona únicamente con fines informativos y no debe considerarse como asesoramiento jurídico para el cumplimiento de DORA y NIS2. ManageEngine no ofrece ninguna garantía, expresa, implícita o legal, en relación con la información contenida en este material. Póngase en contacto con su asesor jurídico para saber cómo afectan DORA y NIS2 a su organización y qué debe hacer para cumplir con
DORA y NIS2.

ManageEngine
una división de **Zoho** Corp.

Para más información:
**www.manageengine.com/latam | latam-sales@manageengine.com**