



#A2EXPERTS

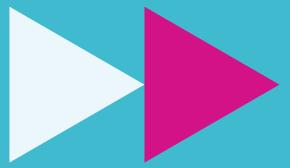
# NORMATIVAS DE CIBERSEGURIDAD A TENER EN CUENTA EN 2025



A2SECURE

Be a master of cybersecurity  
compliance with us!



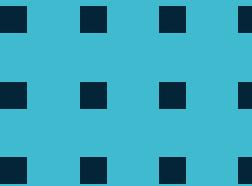


EU

DORA  
NIS2

# DORA/NIS2

NIS2 ya es una realidad, mientras que DORA entrará en vigor el 16 de enero de 2025. Estas dos normativas marcan el inicio de una **nueva era en el ámbito de la normativa en ciberseguridad**.



## ¿Cómo pueden prepararse las empresas?

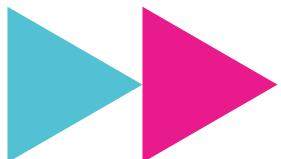
Con ambas normativas el primer paso debe ser analizar el alcance y el impacto en el *corebusiness* de la empresa. En estos casos el **GAP Analysis** es la opción más conveniente.

Posteriormente, lo ideal es definir un Plan de Acción mediante la ayuda de un equipo experto en ciberseguridad.



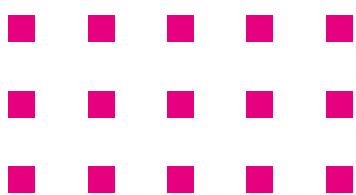
¿Necesitas ayuda para activar tu proceso de adaptación? Contáctanos [info@a2secure.com](mailto:info@a2secure.com)

A2SECURE



# PCI DSS

Aunque casi llevamos un año con la versión 4 de PCI DSS, el **31 de marzo de 2025** muchos de los controles que hasta ahora eran considerados “buenas prácticas” pasarán a ser obligatorios.



## ¿Cómo pueden prepararse las empresas?

Es fundamental disponer de mecanismos para empezar a **cumplir cuanto antes con los 51 controles restantes** - 10 de ellos dirigidos exclusivamente a proveedores-.

De lo contrario, te arriesgarás a obtener una AOC no compliance y pondrás en riesgo tu operatividad dentro del ecosistema de pagos.



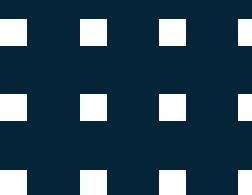
Empieza a planificar tu adaptación a los nuevos controles con un equipo especializado en PCI:  
[info@a2secure.com](mailto:info@a2secure.com)



# ENS

Desde que el 5 de mayo de 2024 empezó a ser obligatorio disponer del certificado de ENS para poder presentarse a concursos y licitaciones públicas, las empresas empezaron a ponerse las pilas para lograr cumplir con el estándar.

No disponer del ENS limita tus oportunidades de negocio y la posibilidad de trabajar con la Administración Pública.



## ¿Cómo pueden prepararse las empresas?

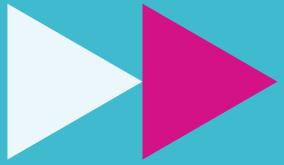
Lo primero que deben hacer es llevar a cabo una **evaluación de riesgos y vulnerabilidades y comenzar a implementar las medidas**. Además, es importante realizar auditorías y evaluaciones regulares.

El proceso de certificación del ENS es bastante complejo, por lo que es preferible contar con la ayuda de una consultora de ciberseguridad para agilizarlo y prevenir cualquier error.



¿Te gustaría obtener tu certificación del ENS?  
Escríbenos a [info@a2secure.com](mailto:info@a2secure.com)

A2SECURE



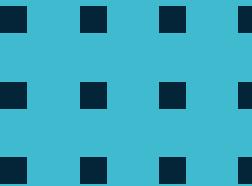
Authorized Signature

Not Valid Unless Signed

9999 999

# PSD 3

La PSD 3 es una Directiva de la UE que establece normas para la autorización y supervisión de los proveedores de servicios de pago no bancarios en la Unión Europea. La normativa incluye nuevos requisitos en la autenticación reforzada de clientes y aborda los protocolos bancarios abiertos.



## ¿Cómo pueden prepararse las empresas?

Si eres una compañía vinculada al ecosistema de pagos te recordamos que **cumplir con la PSD2 no es suficiente**. Es importante establecer una hoja de ruta para abordar los cambios más importantes de la PSD3.



¿Necesitas ayuda para activar tu proceso de adaptación? Contáctanos [info@a2secure.com](mailto:info@a2secure.com)

A2SECURE