

# Autoevaluación DORA en 10 Puntos

a  
 **PRIVALEX**  
checklist



**La Digital Operational Resilience Act (DORA)** ya está plenamente en vigor y está diseñada para garantizar que bancos, aseguradoras, empresas de inversión y sus proveedores TIC puedan resistir y recuperarse de interrupciones digitales.

**Para las entidades financieras, el cumplimiento no es opcional. Pero ¿por dónde empezar?**

Esta autoevaluación en 10 puntos te ayuda a comparar rápidamente tu nivel de preparación frente a los requisitos fundamentales de DORA.

## **BENEFICIOS DE CUMPLIR CON DORA**

### **MAYOR RESILIENCIA Y CONTINUIDAD OPERATIVA**

La implementación de DORA permite anticipar, resistir y recuperarse rápidamente de ciberataques, fallos tecnológicos e interrupciones, protegiendo la estabilidad del negocio

### **VENTAJA COMPETITIVA EN EL SECTOR FINANCIERO**

Demostrar el cumplimiento de DORA refuerza la reputación ante clientes, reguladores e inversores, posicionando a la empresa como un socio tecnológico y financiero de confianza

### **ACCESO AL MERCADO Y CUMPLIMIENTO REGULATORIO**

Cumplir con DORA garantiza la alineación regulatoria en toda la UE, evitando sanciones y asegurando el acceso a contratos y operaciones dentro del sistema financiero europeo

## **EVALUANDO TU NIVEL DE PREPARACIÓN**

**8-10 "Sí": Preparación sólida.**

*Estás bien encaminado; solo necesitas validar los detalles.*

**4-7 "Sí": Preparación moderada.**

*Las vulnerabilidades significativas podrían retrasar el cumplimiento.*

**0-3 "Sí": Riesgo elevado.**

*Se requiere acción inmediata para evitar exposición regulatoria y contractual.*



## 1 Gobernanza y Responsabilidad

¿La gestión del riesgo TIC y ciber está supervisada por el consejo de administración y la alta dirección, con una responsabilidad claramente definida?

*Sí, implementado*

*Parcial*

*No implementado*

## 2 Marco de Gestión de Riesgos TIC

¿Dispones de un marco documentado para identificar, evaluar y mitigar los riesgos TIC en toda la organización?

*Sí, implementado*

*Parcial*

*No implementado*

## 3 Respuesta y Notificación de Incidentes

¿Puedes detectar, clasificar y notificar los incidentes TIC graves a los reguladores dentro de los plazos establecidos?

*Sí, implementado*

*Parcial*

*No implementado*

## 4 Continuidad de Negocio y Recuperación

¿Mantienes planes de continuidad de negocio y recuperación ante desastres, probados regularmente, que cubran interrupciones TIC?

*Sí, implementado*

*Parcial*

*No implementado*

## 5 Pruebas de Resiliencia Operativa Digital

¿Realizas pruebas periódicas de penetración y pruebas avanzadas de resiliencia (por ejemplo, pruebas basadas en amenazas para funciones críticas)?

*Sí, implementado*

*Parcial*

*No implementado*

## 6 Gestión de Riesgos de Terceros

¿Evalúas y supervisas la resiliencia de los proveedores críticos de servicios TIC (por ejemplo, cloud, SaaS, externalización)?

*Sí, implementado*

*Parcial*

*No implementado*

## 7 Garantías Contractuales

¿Incluyen tus contratos con proveedores TIC las cláusulas obligatorias exigidas por DORA (derechos de acceso, gestión de datos, terminación, obligaciones de notificación)?

*Sí, implementado*

*Parcial*

*No implementado*

## 8 Intercambio de Información

¿Participas en acuerdos sectoriales de intercambio de información para compartir inteligencia sobre ciberamenazas y buenas prácticas?

*Sí, implementado*

*Parcial*

*No implementado*

## 9 Auditoría y Supervisión

¿Están tus prácticas de gestión de riesgos TIC y resiliencia completamente documentadas, son auditables y están sujetas a una revisión independiente?

*Sí, implementado*

*Parcial*

*No implementado*

## 10 Roadmap de Cumplimiento

¿Tienes un responsable designado para DORA, un análisis de brechas y una hoja de ruta para cumplir con los requisitos?

*Sí, implementado*

*Parcial*

*No implementado*

# PRÓXIMOS PASOS

We're seeing financial firms struggling to understand DORA, especially around third-party risk and testing requirements. A structured self-assessment like this is the fastest way to identify gaps.

At PrivaLex Partners, we help firms translate DORA into actionable roadmaps aligned with ISO 27001, NIS2, and sector best practices.

**CONTÁCTANOS**

**SI ESTÁS INTERESADO EN ALCANZAR EL CUMPLIMIENTO CON DORA CON**

