foliume

GUÍA PRÁCTICA PARA CORREDURÍAS

¿Cómo afecta DORA *a la mediación de seguros*?

Qué es el Reglamento de resiliencia operativa digital, a quién aplica de verdad, los siete pilares de cumplimiento, las sanciones y por dónde empezar, sin volverte loco.

Guía de Foliume | Edición 2025 | Lectura de 5 minutos

DORA (Digital Operational Resilience Act) es una regulación europea que busca reforzar la seguridad tecnológica en todo el ecosistema financiero, incluidas aseguradoras, grandes grupos de mediación y proveedores TIC.

Su objetivo no es evitar los ciberataques, sino minimizar su impacto y garantizar que las operaciones continúen con normalidad incluso durante fallos o incidentes.

01 ALCANCE

¿A quién aplica *y a quién no*?

APLICA A

- Aseguradoras y reaseguradoras.
- Grandes grupos de mediación, de más de 250 empleados.
- Proveedores TIC críticos.

NO APLICA A

- Corredores y agentes de seguros con menos de 250 empleados. No se aplica directamente a los pequeños corredores, pero conviene tenerlo en cuenta por sus implicaciones indirectas.

Ciberseguridad: una prioridad ineludible

- Los ataques son cada vez más sofisticados y frecuentes.
- Ya en 2013 se producía un ataque cada 39 segundos, según Cybersecurity Ventures.
- La resiliencia digital es esencial para asegurar la continuidad del negocio.

02 PILARES

Los siete pilares clave *de cumplimiento*

01 **Gestión de riesgos TIC**

Marco sólido para anticipar, mitigar y supervisar riesgos tecnológicos.

02 **Gestión de incidentes tecnológicos**

Registro, clasificación y notificación obligatoria de incidentes graves a las autoridades.

03 **Pruebas de resiliencia operativa**

Simulacros, test de penetración y auditorías para validar la robustez de los sistemas.

04 **Gestión del riesgo de terceros TIC**

Supervisión contractual y técnica sobre proveedores externos.

05 **Intercambio de información**

Colaboración con otras entidades para compartir inteligencia sobre ciberamenazas.

06 **Supervisión a proveedores TIC críticos**

Vigilancia directa de las autoridades europeas cuando se trate de actores sistémicos.

07 **Gobernanza y responsabilidad de la alta dirección**

Implicación activa del consejo en la estrategia de resiliencia digital.

03 OBLIGACIONES

Las cinco obligaciones para aseguradoras *y mediadores grandes*

01 **Marco de gestión de riesgos tecnológicos**

Protocolos claros, roles definidos y medidas de control documentadas.

02 **Pruebas de resistencia y auditorías de vulnerabilidad**

Validar periódicamente que los sistemas resisten ataques y fallos.

03 **Gestión y notificación de incidentes**

Reportar los incidentes graves a las autoridades en menos de 24 horas.

04 **Supervisión de terceros TIC**

Contratos ajustados a DORA y vigilancia continua sobre proveedores.

05 **Formación y concienciación interna**

Imprescindible involucrar a todo el personal, técnico y no técnico.

Sanciones por incumplimiento

- Multas económicas proporcionales, de hasta el 2 % de la facturación anual.

- Sanciones penales en los casos graves.
- Restricciones operativas por parte del regulador.

04 QUÉ HACER

Oportunidades, retos *y por dónde empezar*

OPORTUNIDADES

- Ventaja competitiva para quienes se anticipen.
- Confianza del cliente ante la mejora en ciberseguridad.
- Impulso a la digitalización profesional del sector.
- Servicios nuevos vinculados a la ciberseguridad: auditorías, seguros cibernéticos, asesoría.
- Mayor colaboración entre empresas.

RETOS PARA LA MEDIACIÓN

- Trasladar obligaciones a terceros tecnológicos.
- Dificultad para estandarizar contratos TIC conforme a DORA.
- Costes de implantación para pymes.
- Falta de talento especializado en ciberseguridad.
- Notificaciones a clientes y autoridades en plazos muy ajustados.

Herramientas clave para cumplir

- Plataformas de gestión de riesgos TIC.
- Sistemas de detección y respuesta a incidentes.
- Automatización de informes regulatorios.
- Soluciones de auditoría y escaneo de vulnerabilidades.
- Formación continua para los equipos internos.

Recomendaciones prácticas

01 **Haz un diagnóstico de brechas**

Un gap analysis para saber dónde estás respecto a lo que exige DORA.

02 **Inicia un plan de adaptación por fases**

No hace falta resolverlo todo de golpe.

03 **Implica a la alta dirección y a los responsables legales**

La gobernanza es uno de los pilares.

04 **Revisa y renegocia los contratos con proveedores TIC**

Son el eslabón que DORA mira con más atención.

05 **Apuesta por la formación como eje de resiliencia**

Técnicos y no técnicos.

CONCLUSIÓN

DORA no va de evitar ataques, *va de seguir operando*

Aunque no te aplique directamente, el reglamento marca el estándar con el que las compañías y los grandes grupos van a medir a sus proveedores y a sus socios de distribución.

Anticiparse es una ventaja competitiva: mejora la confianza del cliente y profesionaliza la operativa.

Diagnóstico, plan por fases, contratos revisados y formación. Con eso empiezas.

foliume

La guía te dice qué hacer. *Foliume* lo hace contigo.

Tu equipo y los agentes de IA en el mismo tablero para cotizar, atender y gestionar directamente con las compañías. Tú apruebas, Wilfredo ejecuta.

Conocer Wilfredo →

Más recursos