GRCForce

Guía práctica de integración regulatoria europea

24 de junio de 2026

grcforce.com/es/#contact

Practical governance, risk and compliance guidance for European organisations.

Un único modelo operativo para NIS2, DORA, ISO 27001 y TISAX

Un marco práctico para organizaciones europeas que necesitan una única columna vertebral de gobernanza en lugar de cuatro programas de cumplimiento separados.

Objetivo: Integrar NIS2, DORA, ISO 27001 y TISAX en un único modelo operativo, reduciendo la duplicación de evidencias, la fragmentación de los informes y los programas locales paralelos.

A quién va dirigida: CISOs, responsables de GRC, directores de riesgos y responsables de cumplimiento de organizaciones europeas medianas y grandes con operaciones en varios países.

Enfoque: Definir una filosofía común de controles y documentar requisitos locales adicionales únicamente cuando la legislación o las orientaciones del regulador sean realmente diferentes.

Matriz de integración regulatoria

Mapee cada dominio de control una sola vez y, a continuación, determine la base común y las adaptaciones justificadas.

Dominio	NIS2	DORA	ISO 27001	TISAX
Gobernanza	Responsabilidad del consejo, supervisión de la dirección y claridad de funciones	Responsabilidad del órgano de dirección sobre el riesgo TIC y la resiliencia	Compromiso del liderazgo, alcance del SGSI y propiedad de los controles	Gobernanza de la seguridad de la información para generar confianza en el sector de automoción
Evaluación de riesgos	Medidas de gestión de riesgos para entidades esenciales e importantes	Marco de gestión del riesgo TIC y conocimiento de escenarios	Metodología de evaluación y tratamiento de riesgos	Clasificación de riesgos alineada con las expectativas de los socios
Notificación de incidentes	Clasificación de incidentes significativos y plazos de notificación	Clasificación, escalado y notificación de incidentes TIC graves	Proceso de incidentes, evidencias y mejora	Gestión de incidentes de seguridad y lógica de notificación a clientes
Riesgo de terceros	Supervisión del riesgo de seguridad de proveedores y prestadores de servicios	Ciclo de vida del riesgo de terceros TIC y disciplina del registro	Controles de relaciones con proveedores y evidencias de aseguramiento	Controles de proveedores incluidos en el alcance TISAX
Pruebas	Pruebas de seguridad adecuadas al riesgo y la criticidad	Pruebas de resiliencia operativa digital y remediación	Auditoría interna, seguimiento y pruebas de controles	Evidencias de evaluación y remediación guiada por la madurez
Documentación y evidencias	Políticas, medidas y evidencias que demuestren la diligencia debida	Registros, informes, resultados de pruebas y evidencias para el consejo	Registros del SGSI, evidencias de controles y trazas de auditoría	Artefactos preparados para evaluación y paquetes de evidencias
Adaptaciones locales	Transposición nacional y expectativas de la autoridad competente	Expectativas sectoriales y de supervisión cuando proceda	Alcance local de certificación o requisitos jurídicos adicionales	Requisitos específicos del cliente o del mercado de automoción

Cómo utilizar la guía

1. Seleccione un dominio de control, por ejemplo control de accesos, notificación de incidentes o gobernanza de proveedores.
2. Recoja las obligaciones vigentes de cada regulación o marco.
3. Defina una única política base y un conjunto de controles que satisfaga el requisito más exigente.
4. Documente adaptaciones locales solo cuando la legislación, las orientaciones del regulador o las expectativas del cliente sean realmente diferentes.
5. Acuerde una evidencia una sola vez, mapéela con todos los marcos y reutilícela.

Errores habituales que deben evitarse

- Cuatro plantillas de evaluación de riesgos diferentes
- Definiciones de incidente distintas para cada regulación
- Equipos locales que crean políticas paralelas en lugar de adaptaciones
- Programas estáticos que nunca revisan los mapeos cuando cambian las orientaciones

Siguiente paso

Utilice esta matriz en un breve taller de integración regulatoria. Para evaluar su modelo actual, contacte con GRCForce y solicite una Revisión de Integración Regulatoria específica en https://grcforce.com/es/#contact.

GRCForce | Gobernanza, riesgo y cumplimiento prácticos para organizaciones europeas | grcforce.com