GRCForce

Lista de comprobación para auditar contratos de proveedores conforme a NIS2 y DORA

15 de junio de 2026

grcforce.com/es/#contact

Practical governance, risk and compliance guidance for European organisations.

Publicado el 15 de junio de 2026 | GRCForce

Utilice esta lista para comprobar si los contratos con sus proveedores críticos respaldan una resiliencia operativa real, y no solo la finalización del proceso de compras.

Está diseñada para organizaciones que revisan relaciones materiales con terceros de TIC, servicios cloud, SaaS, servicios gestionados y otros proveedores incluidos en el ámbito de NIS2 y/o DORA.

Cómo utilizar esta lista

Para cada cláusula o pregunta, marque una de las siguientes opciones:

- Implantada y adecuada
- Cubierta parcialmente
- Ausente
- Requiere revisión jurídica

Un contrato no necesita tener una redacción perfecta desde el primer día. Sí necesita que las carencias tengan un responsable claro y que exista una decisión documentada sobre si el riesgo es aceptable.

12 cláusulas y preguntas contractuales que deben revisarse

1. Derecho de auditoría

¿Otorga el contrato a su organización un derecho práctico a obtener evidencias de auditoría, revisar informes de controles y solicitar medidas de seguimiento cuando se detecten deficiencias significativas?

Por qué es importante: si no puede comprobar o revisar de forma creíble los controles del proveedor, está confiando en declaraciones y no en garantías verificables.

2. Obligaciones de seguridad

¿Se establecen claramente las obligaciones mínimas de seguridad del proveedor, incluida la protección de sistemas, el control de accesos, la gestión de vulnerabilidades, el registro de actividad, las copias de seguridad, la recuperación y la gestión segura de cambios?

Por qué es importante: las referencias vagas a una «seguridad conforme a los estándares del sector» suelen ser demasiado débiles cuando se produce un incidente.

3. Plazo de notificación de incidentes

¿Define el contrato con qué rapidez debe notificarle el proveedor un incidente de seguridad, una interrupción del servicio, una brecha de datos o un fallo material de control?

Por qué es importante: expresiones como «sin dilación indebida» suelen ser demasiado imprecisas para servicios críticos. Se necesitan plazos operativamente útiles.

4. Control de accesos e identidades

¿Define el contrato cómo se gestiona el acceso privilegiado, cómo se revisan las cuentas y cómo se revoca el acceso cuando una persona abandona la organización o cuando finaliza el servicio?

Por qué es importante: muchos incidentes de proveedores comienzan con accesos administrativos débiles y una gestión deficiente de identidades.

5. Transparencia sobre ubicación y tratamiento de datos

¿Puede identificar dónde se tratan, almacenan, respaldan y consultan sus datos, incluido el uso de subcontratistas o equipos de soporte ubicados en otros países?

Por qué es importante: la resiliencia y la exposición regulatoria son más difíciles de gestionar cuando el tratamiento de datos es opaco.

6. Control de subcontratistas

¿Necesita el proveedor su aprobación, o al menos una notificación previa, antes de incorporar subcontratistas materiales que puedan afectar a la prestación del servicio, la seguridad o el cumplimiento?

Por qué es importante: el riesgo de cuarta parte suele aparecer a través de dependencias ocultas que nunca fueron evaluadas.

7. Continuidad de negocio y recuperación ante desastres

¿Exige el contrato que el proveedor mantenga y pruebe medidas de continuidad de negocio y recuperación ante desastres adecuadas a la criticidad del servicio?

Por qué es importante: la resiliencia no es una declaración. Requiere objetivos de recuperación, procedimientos probados y evidencias.

8. Niveles de servicio vinculados a la criticidad

¿Están los niveles de servicio, los tiempos de recuperación, los compromisos de soporte y las vías de escalado alineados con la importancia real del servicio para el negocio?

Por qué es importante: muchos contratos están redactados como si el servicio fuera rutinario, incluso cuando sostiene un proceso crítico.

9. Devolución, extracción y eliminación de datos

¿Explica el contrato cómo se devolverán sus datos, en qué formato, dentro de qué plazo, con qué coste y cómo se eliminarán los datos residuales al finalizar la relación?

Por qué es importante: si las condiciones de salida no están claras, puede quedar bloqueado operativamente.

10. Cláusulas de cambio de control y cambios materiales

¿Le protege el contrato si el proveedor es adquirido, cambia de forma sustancial su modelo de servicio, traslada operaciones o sustituye subcontratistas clave?

Por qué es importante: el riesgo del proveedor puede cambiar de un día para otro sin que se produzca ningún cambio en su organización.

11. Obligaciones de evidencia e información

¿Debe el proveedor aportar periódicamente evidencias como informes de auditoría, resultados de pruebas, certificaciones, actualizaciones de riesgos o declaraciones sobre la eficacia de los controles?

Por qué es importante: una diligencia debida realizada una sola vez no es suficiente para relaciones críticas.

12. Apoyo a la salida y asistencia en la transición

¿Exige el contrato que el proveedor apoye la transición a otro proveedor o a un servicio interno mediante cooperación, documentación y asistencia técnica?

Por qué es importante: la resiliencia incluye la capacidad de abandonar una relación sin una interrupción grave.

Señales de alerta que requieren atención inmediata

- Ausencia de derecho de auditoría, o redacción que deja la auditoría enteramente a discreción del proveedor
- Ausencia de un plazo claro de notificación de incidentes
- Ausencia de una cláusula sobre cambios de subcontratistas
- Ausencia de un compromiso de recuperación probado para servicios críticos
- Ausencia de condiciones prácticas para la extracción o eliminación de datos
- Ausencia de obligaciones de apoyo a la salida
- Ausencia de obligación de aportar evidencias de aseguramiento actualizadas
- Ausencia de protección ante cambios de control

Guía rápida de puntuación

- Entre 10 y 12 elementos implantados y adecuados: base contractual sólida
- Entre 7 y 9 elementos implantados: base viable, aunque deben revisarse las carencias prioritarias
- Entre 4 y 6 elementos implantados: riesgo contractual elevado
- Entre 0 y 3 elementos implantados: el contrato debe considerarse de alta prioridad para su remediación

Casos de uso recomendados

Esta lista resulta útil para:

- Revisiones de incorporación de proveedores
- Revisiones de renovación contractual
- Evaluaciones de terceros TIC conforme a DORA
- Revisiones del riesgo de proveedores conforme a NIS2
- Talleres de alineamiento entre compras y asesoría jurídica
- Informes al consejo o a la dirección sobre resiliencia de terceros

Fuentes oficiales de referencia

Fuentes de la Unión Europea

- Texto oficial de la Directiva NIS2 en EUR-Lex: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Texto oficial del Reglamento DORA en EUR-Lex: https://eur-lex.europa.eu/eli/reg/2022/2554/oj
- Página de la Comisión Europea sobre actos de ejecución y delegados de DORA: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en
- Página de ESMA sobre DORA: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- Página de la Comisión Europea sobre la implantación de NIS2 en Bélgica: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Fuentes belgas

- Portal de información NIS2 del Centre for Cybersecurity Belgium: https://belgium-nis2.be/en/
- Sitio principal del Centre for Cybersecurity Belgium: https://ccb.belgium.be/en
- Punto de contacto CERT.be mediante la página de la Comisión Europea sobre la implantación en Bélgica: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive-belgium

Bloque breve para publicaciones o barras laterales de artículos

Fuentes oficiales útiles para trabajar con NIS2 o DORA:

- Texto oficial de NIS2: Directiva (UE) 2022/2555 en EUR-Lex
- Texto oficial de DORA: Reglamento (UE) 2022/2554 en EUR-Lex
- Visión general y novedades de DORA: ESMA
- Implantación de NIS2 y puntos de contacto en Bélgica: página de Estrategia Digital de la Comisión Europea
- Información práctica sobre NIS2 en Bélgica: Centre for Cybersecurity Belgium

Apoyo para una revisión práctica

Contacte con GRCForce para revisar dónde están desalineadas la redacción contractual de proveedores, la gobernanza y la resiliencia operativa: https://grcforce.com/es/#contact

Esta lista ofrece orientación práctica y no sustituye al asesoramiento jurídico. La redacción contractual y la interpretación regulatoria deben elevarse a la revisión jurídica correspondiente.