NIS 2 ART. 21(2)(D)

Cuestionario para proveedores NIS 2

Un cuestionario abierto y anclado en el derecho de la UE para la evaluación de proveedores conforme a NIS 2

Perfil del proveedor	18 campos
Prácticas de seguridad	26 campos
Específico de SaaS	5 campos
Específico de On-Premise	4 campos
Professional Services	3 campos
Managed Services	3 campos

Cada campo está anclado a una fuente primaria de nivel europeo: NIS 2 Art. 21(2), CIR 2024/2690, ENISA Technical Implementation Guidance, GDPR Art. 28 o el Cyber Resilience Act. Los complementos sectoriales (TISAX, VDA ISA, BSI C5, KRITIS) se añaden a esta base.

Fuente: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

Licencia: MIT (esquema) + CC BY 4.0 (contenido). Libre para usar, bifurcar y adaptar.

1. Perfil del proveedor

18 campos

Razón social

STRING · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2

El nombre registrado de su empresa, tal como aparece en el registro mercantil. Ejemplo: Müller GmbH o Acme Software Ltd.

Domicilio social

STRING · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2

El domicilio comercial registrado de su empresa. Basta con una dirección, aunque tenga varias ubicaciones.

País

COUNTRY · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2

El país donde su empresa está legalmente establecida. Dos letras, por ejemplo DE para Alemania.

Dominio principal

URL · OPCIONAL · BASE JURÍDICA: ENISA TIG §5.2(B)

Su dominio principal, normalmente la URL de su sitio web. Ejemplo: acmesoftware.com.

Eslogan (una línea, visible para el cliente)

STRING · OPCIONAL · BASE JURÍDICA: ENISA TIG §5.2(B)

Una línea que resume lo que ofrece. Los clientes la ven en su perfil de proveedor. Ejemplo: ERP para la fabricación de pymes.

Descripción pública (más extensa)

TEXT · OPCIONAL · BASE JURÍDICA: ENISA TIG §5.2(B)

Dos o tres frases sobre su empresa y lo que hace. Esto aparece en su perfil de proveedor. Argumento de venta, postura de seguridad o ambos.

Descripción de los servicios prestados

TEXT · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2(B) + §5.1.4 TIPS

Un párrafo sobre lo que su empresa entrega técnicamente a los clientes. Productos, módulos o servicios concretos. Evite el lenguaje puramente comercial.

Países / regiones donde se tratan los datos de los clientes

STRING · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.4 TIPS

Todos los países donde se almacenan o tratan los datos de sus clientes. Separados por comas, códigos de país ISO. Ejemplo: DE, NL, US. Si trata los datos enteramente dentro de la UE, basta con enumerar los países de la UE.

Nombre del contacto de seguridad

STRING · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(D)

La persona a la que los clientes contactan cuando se produce un incidente de seguridad. En las empresas más pequeñas suele ser el director general o el responsable de TI. Basta con una persona.

Correo electrónico de contacto para incidentes

EMAIL · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(D)

Dirección de correo electrónico que los clientes utilizan para notificar un incidente de seguridad. Idealmente una lista de distribución como security@example.com que llegue a varias personas.

Teléfono de contacto para incidentes (24/7)

PHONE · OPCIONAL · BASE JURÍDICA: CIR 2024/2690 §5.1.4(D)

Número de teléfono para las notificaciones urgentes de incidentes. Si no dispone de guardia 24/7, indique su horario laboral entre paréntesis.

SLA de notificación de incidentes (horas)

INTEGER · OPCIONAL · BASE JURÍDICA: NIS2 ART. 23

Horas desde la detección de un incidente hasta la notificación al cliente, como máximo. Autoevaluación realista, no aspiracional. Valores habituales: 24, 48 o 72 horas.

ID de registro BSI (solo si su empresa está regulada por NIS2)

STRING · OPCIONAL · BASE JURÍDICA: ENISA TIG §5.1.2

Si su empresa está sujeta a NIS 2 y registrada ante el BSI, introduzca aquí el ID de registro. Opcional. Permite a los clientes ver de un vistazo que cumple la misma obligación que una entidad regulada.

Ofrecemos servicios SaaS / alojados

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2(B)

Ejecuta software para los clientes en su propia infraestructura y lo entrega a través de internet. Marque más de una casilla si ofrece varios modelos.

Entregamos software on-premise

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2(B)

Entrega software que los clientes instalan y ejecutan en su propia infraestructura.

Ofrecemos servicios profesionales / consultoría

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2(B)

Su entregable principal es trabajo humano: consultoría, implementación, formación, auditoría o personalización.

Ofrecemos servicios gestionados / MSP

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.2(B)

Opera para el cliente partes de su TI, con personal propio. Típico de los modelos MSP y MSSP.

Utilizamos, integramos o proporcionamos sistemas de IA

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(D)

¿Sus productos o servicios tratan datos de los clientes mediante un modelo de IA o ML? Incluye modelos externos a los que llama a través de una API, por ejemplo OpenAI o Anthropic.

2. Prácticas de seguridad

26 campos

Sistema de gestión de la seguridad de la información documentado (ISMS)

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.2(A)

Marque sí si dispone de una política escrita de seguridad de la información con roles asignados, revisiones periódicas y gestión documentada de incidentes. Una certificación ISO 27001 o BSI Grundschutz implica sí.

Disponer de certificación ISO 27001, BSI Grundschutz o equivalente

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.2(B)

Marque sí si su empresa dispone actualmente de una certificación ISO 27001, BSI Grundschutz, SOC 2 Type II o equivalente. Suba el certificado en la pestaña Certificaciones.

Formación anual de concienciación en seguridad para todo el personal

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(B)

Marque sí si cada miembro del personal recibe al menos una formación anual de concienciación en seguridad de la información. El e-learning cuenta; las simulaciones de phishing se suman.

Verificación de antecedentes del personal con acceso a datos de clientes

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(C)

Marque sí si realiza una verificación de antecedentes al personal con acceso a los datos de los clientes. Nivel habitual: certificado de antecedentes penales o documento equivalente en la contratación.

Proceso documentado de gestión de vulnerabilidades y aplicación de parches

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(F)

Marque sí si dispone de un proceso escrito para gestionar las vulnerabilidades de seguridad: detectar, evaluar, priorizar, parchear o mitigar. La supervisión de CVE y la aplicación de parches basada en SLA son el estándar.

Aceptar el derecho de auditoría del cliente (o proporcionar informes de auditoría)

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(E)

Marque sí si concede a los clientes un derecho de auditoría in situ o les proporciona informes de auditoría sustitutivos (por ejemplo SOC 2, ISAE 3402).

Uso de subencargados / subproveedores

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(G)

Marque sí si recurre a otras empresas para prestar su servicio que tienen acceso a los datos o la infraestructura de los clientes. Ejemplos típicos: AWS, Azure, Cloudflare, Stripe.

Lista de subencargados

TEXT · CONDICIONAL · BASE JURÍDICA: CIR 2024/2690 §5.1.4(G)

Enumere cada subencargado con su nombre, lugar de tratamiento y lo que hace por usted. Basta con una tabla o una lista de viñetas. Actualícela cada vez que añada o elimine uno.

Comprometerse a devolver / destruir los datos del cliente al finalizar el contrato

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: CIR 2024/2690 §5.1.4(H)

Marque sí si se compromete contractualmente a devolver o destruir los datos del cliente al finalizar el contrato. Práctica habitual: exportar y devolver, y luego eliminar en un plazo de 30 días.

Contrato estándar de tratamiento de datos (DPA) disponible

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: GDPR ART. 28

Marque sí si dispone de un contrato estándar de tratamiento de datos conforme al artículo 28 del GDPR que los clientes puedan firmar. Obligatorio en cuanto trate datos personales.

Las políticas de seguridad se revisan al menos una vez al año

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(A) / ENISA TIG §1.1

Marque sí si sus políticas de seguridad se revisan al menos una vez al año y se actualizan según sea necesario. Una nota escrita en el documento basta como prueba.

Plan de respuesta a incidentes documentado

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(B) / ENISA TIG §3

Marque sí si dispone de un plan escrito para gestionar los incidentes de seguridad: quién decide, quién comunica, quién documenta. Al menos un ejercicio de simulación al año es una buena práctica.

Plan de continuidad de negocio / recuperación ante desastres documentado

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(C) / ENISA TIG §4

Marque sí si dispone de un plan que explique cómo mantiene el funcionamiento o se recupera con rapidez durante una interrupción: sistemas críticos, alternativas, objetivos RTO y RPO.

Política de criptografía documentada

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Marque sí si ha documentado por escrito qué criptografía usa y dónde: datos en tránsito (TLS 1.2+), datos en reposo (AES-256), gestión de claves, algoritmos de hash.

Gestión de accesos privilegiados (PAM) para el personal interno

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Marque sí si los administradores y las cuentas privilegiadas cuentan con controles adicionales: inicio de sesión separado, MFA, registro de sesiones o acceso just-in-time.

MFA obligatorio para todas las cuentas internas de administración / privilegiadas

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(J)

Marque sí si cada cuenta interna de administración o privilegiada debe usar MFA. Los tokens de hardware o las aplicaciones de autenticación cuentan; los SMS no.

Mantener un inventario de activos de información

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(I) / ENISA TIG §12.4

Marque sí si mantiene una lista actualizada de cada sistema de información que utiliza para prestar su servicio: servidores, bases de datos, herramientas SaaS, endpoints. Basta con una hoja de cálculo.

Programa de pruebas de penetración anual o bienal

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: NIS2 ART. 21(2)(E) / ENISA TIG §6.5

Marque sí si encarga una prueba de penetración externa al menos cada uno o dos años. Para las empresas más pequeñas, un escaneo de vulnerabilidades externo como paso mínimo es aceptable.

Divulgamos los eventos de ciberseguridad notificables pasados cuando los clientes lo solicitan

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.2

Marque sí si, a petición del cliente, divulga abiertamente si su empresa tuvo en el pasado incidentes de seguridad notificables y cuáles. Ventana habitual: los últimos tres a cinco años.

Prestar asistencia a los clientes en caso de incidente sin coste / a coste predefinido

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.4 TIPS

Marque sí si se compromete a ayudar a los clientes sin coste adicional cuando un incidente es causado por su producto o servicio. Si en su lugar acuerda de antemano una tarifa diaria predefinida, marque también sí.

Cooperar plenamente con las autoridades competentes (BSI, ENISA, CSIRT nacionales)

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.4 TIPS

Marque sí si se compromete a cooperar plenamente con las autoridades competentes como el BSI, la ENISA o los CSIRT nacionales durante las inspecciones, las auditorías y la gestión de incidentes. Estándar para los proveedores serios.

Notificar a los clientes cualquier cambio sustancial que afecte a la prestación del servicio

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.4 TIPS

Marque sí si se compromete a notificar a los clientes cualquier cambio sustancial que afecte a su capacidad de prestar el servicio: adquisiciones, cambios de subencargado, cambios técnicos importantes.

Notificar a los clientes con antelación si cambian los lugares de tratamiento de datos

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.4 TIPS

Marque sí si informa a los clientes con antelación antes de que cambie el lugar de tratamiento de sus datos. Importante para la protección de datos y para una supervisión de la cadena de suministro conforme al GDPR.

Estrategia de salida documentada con periodo de transición obligatorio

BOOLEAN · OBLIGATORIO · BASE JURÍDICA: ENISA TIG §5.1.4 TIPS

Marque sí si dispone de una estrategia de salida escrita: cuánto dura un traspaso ordenado, qué datos y conocimientos se transfieren, a qué se compromete durante la transición.

Proporcionar un SBOM-for-AI según los elementos mínimos del G7

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(D) / ENISA TIG §5.1.2

Opcional. Marque sí si puede proporcionar un SBOM-for-AI según los elementos mínimos del G7 (mayo de 2026). Documenta metadatos, modelos, datos de entrenamiento, infraestructura, propiedades de seguridad, KPI y comportamiento del sistema. Estándar voluntario.

URL del documento SBOM-for-AI

URL · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(D) / ENISA TIG §5.1.2

URL pública o compartida de su documento SBOM-for-AI. Puede ser un PDF, un archivo JSON o una página de proyecto.

3. Específico de SaaS

5 campos

Región de alojamiento

STRING · CONDICIONAL · BASE JURÍDICA: ENISA TIG §5.2

La región de la nube donde se alojan los datos de los clientes. Ejemplo: AWS eu-central-1, Azure West Europe. Indique la región principal; las regiones secundarias o de respaldo pueden añadirse separadas por comas.

Cifrado en reposo

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Marque sí si los datos de los clientes en disco están cifrados en reposo con AES-256 o equivalente. El cifrado de disco gestionado por la nube (AWS EBS, Azure Disk Encryption) cuenta.

Cifrado en tránsito (TLS ≥ 1.2)

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(H) / ENISA TIG §9

Marque sí si todos los puntos de acceso orientados al cliente exigen TLS 1.2 o superior. Se prefiere TLS 1.3. El HTTP simple debe redirigir a HTTPS.

MFA obligatorio para todas las cuentas de administración

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(J) / ENISA TIG §11.3

Marque sí si cada cuenta de administración interna en la plataforma SaaS debe usar MFA. El mismo estándar que su política de administración interna.

Objetivo de tiempo de recuperación (RTO) en horas

INTEGER · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(C) / ENISA TIG §4

Número máximo de horas que su servicio puede estar no disponible antes de la recuperación. Valor de SLA realista, no aspiracional. Valores habituales de SaaS: 4, 8 o 24 horas.

4. Específico de On-Premise

4 campos

Proporcionar una lista de materiales de software (SBOM)

BOOLEAN · CONDICIONAL · BASE JURÍDICA: CRA / NIS2 ART. 21(2)(D)

Marque sí si entrega una lista de materiales de software (SBOM) con cada versión. CycloneDX o SPDX son los formatos estándar. Obligatorio en virtud del Cyber Resilience Act para los productos introducidos en el mercado de la UE a partir de diciembre de 2027.

Las versiones están firmadas criptográficamente

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(E) / ENISA TIG §6.5

Marque sí si cada artefacto de versión lleva una firma criptográfica que los clientes puedan verificar. Las claves de firma están documentadas y se rotan. Las firmas Sigstore o PGP cuentan ambas.

Política de divulgación de vulnerabilidades publicada

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(E) / ENISA TIG §3

Marque sí si dispone de una vía documentada públicamente para notificar vulnerabilidades de seguridad. Basta con un archivo security.txt en su dominio (conforme a RFC 9116) o un correo electrónico dedicado como security@example.com.

SLA de parches para CVE críticas (horas)

INTEGER · CONDICIONAL · BASE JURÍDICA: CIR 2024/2690 §5.1.4(F)

Horas desde la divulgación pública de una CVE hasta una versión parcheada para las vulnerabilidades críticas (CVSS 9.0+). Compromiso realista, no aspiracional. Valores habituales: 24, 48 o 72 horas.

5. Professional Services

3 campos

Alcance de la verificación de antecedentes

STRING · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(I) / CIR 2024/2690 §5.1.4(C)

Describa cómo evalúa a los consultores para los puestos sensibles. Ejemplo: certificado de antecedentes penales para todos los consultores, además de verificación de referencias para los encargos que impliquen datos clasificados.

NDA firmado con todos los consultores

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.4

Marque sí si cada consultor firma un acuerdo de confidencialidad antes de ser asignado al trabajo con el cliente. Ya sea como parte del contrato laboral o como un NDA independiente.

Política de conducta documentada en las instalaciones del cliente

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Marque sí si dispone de un código de conducta escrito para los consultores que trabajan en las instalaciones del cliente: gestión de credenciales, regla de bloqueo de pantalla, qué hacer si los datos salen del emplazamiento.

6. Managed Services

3 campos

Gestión de accesos privilegiados (PAM) implantada

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(I) / ENISA TIG §11.3

Marque sí si utiliza una herramienta de gestión de accesos privilegiados para las sesiones remotas administrativas en los sistemas de los clientes. Ejemplos: CyberArk, BeyondTrust, Teleport. Una configuración de jump-host con registro de logs cuenta.

Las sesiones de administración se graban

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(F) / ENISA TIG §10

Marque sí si las sesiones de administración en los sistemas de los clientes se graban y se conservan para su revisión. Conservación habitual: de 90 días a 1 año. Necesaria para la reconstrucción forense tras los incidentes.

Cobertura de guardia 24/7

BOOLEAN · CONDICIONAL · BASE JURÍDICA: NIS2 ART. 21(2)(B) / ENISA TIG §3

Marque sí si dispone de una guardia 24/7 que responde a los incidentes de seguridad en los sistemas de los clientes. El soporte limitado al horario laboral no cumple el requisito.