

Preparación para la evaluación NIS2

Guía para dirección e IT • Complementa el cuestionario Excel con respuestas seleccionables

Este material complementa la lista de verificación inicial, ‘¿Se aplica NIS2 a su empresa?’, que sigue sin cambios. Nos ayuda a entender el alcance, las responsabilidades y la situación conocida antes de una evaluación o auditoría. No le pedimos que lleve a cabo investigaciones técnicas para responder.

Qué obtiene en esta fase

Una vista declarada de la situación, la información que necesita aclaración y una base para seleccionar el servicio apropiado. No resulta en una puntuación oficial del DNSC, un certificado o confirmación de cumplimiento.

Cómo completar el archivo

QUIÉN	DÓNDE COMPLETAR	QUÉ SE INDICA
Coordinador de la solicitud	01_Perfil y 05_Plazos	La entidad, volúmenes aproximados, roles de contacto y etapas conocidas.
Dirección / persona designada	02_Direccion — 14 questions	Responsabilidades, actividades críticas, riesgos, decisiones y recursos.
IT interno, proveedor IT o grupo	03_IT — 24 preguntas; 04_Casos_especiales — 6	Existencia de medidas, alcance cubierto y cualquier desconocido.

Tiempo indicativo: 10–15 minutos para la gestión y 15–25 minutos para la TI, más los datos de perfil. Se estiman, no se imponen plazos. Una copia se completa para cada entidad jurídica.

Cinco respuestas, sin largas explicaciones técnicas

Sí — se conoce la situación en todo el alcance pertinente. Parcialmente — solo cubre una parte. No — según la información conocida, la medida no existe. No lo sabemos — no puede confirmarse la información. Posiblemente no aplicable — explique el motivo; la aplicabilidad se validará después.

Completa sólo las células amarillas pálidas. Para ‘Sí’, la evidencia se revisa más adelante. Para ‘Posiblemente no se aplica’, la explicación no constituye una exclusión legal. El resumen cuenta las respuestas; no calcula un porcentaje de cumplimiento.

Qué aclaramos antes de evaluar

El cuestionario separa las decisiones de gestión de la ejecución técnica. Una empresa no se asume conforme simplemente porque tiene una licencia, ni se supone que un proveedor haya asumido que ha asumido el cumplimiento de cada obligación de gestión. [R1-R3]

FUNCIÓN	PREGUNTA CLAVE	EJEMPLOS ORIENTATIVOS
Gobernar — GV	¿Quién decide y supervisa?	Responsabilidades, políticas, riesgos, proveedores, presupuesto e informes.
Identificar — ID	¿Qué debe protegerse?	Activos y aplicaciones conocidos, actividades críticas, vulnerabilidades y dependencias.
Proteger — PR	¿Qué reduce el riesgo?	Acceso, autenticación, dispositivos, datos, formación, copias de seguridad y segmentación.
Detectar — DE	¿Quién detecta los problemas?	Alertas, registros, supervisión de eventos y horario real de vigilancia.
Responder — RS	¿Qué hacemos durante un incidente?	Escalado, decisiones, limitación del impacto, comunicación y conservación de evidencias.
Recuperar — RC	¿Cómo reanudamos la actividad?	Restauración probada, prioridades de recuperación y canales alternativos.

Las seis funciones se toman de la estructura de las medidas DNSC. Las preguntas son nuestra propia síntesis, no una reproducción del catálogo o un sustituto para comprobar todos los controles aplicables. [R3]

Ejemplos del nivel de detalle adecuado

Para la autenticación: ‘Sí, para los administradores de TI; desconocido para todos.’ Para la copia de seguridad: ‘Tenemos copias de seguridad, pero no sabemos cuándo la restauración fue probada por última vez.’ Para un grupo: ‘La seguridad se gestiona centralmente; la persona responsable local puede identificar quién confirma la cobertura.’

No envíe información explotable ni datos de clientes

No introduzca contraseñas, fichas, claves, direcciones IP, configuraciones, listas de usuarios, extractos del sistema o informes de vulnerabilidad. Sólo se solicita la existencia de medidas y el papel que puede confirmarlas.

Las áreas especiales —desarrollo, nube, servicios gestionados, OT/IoT/médico, exposición pública y entorno físico— se aclaran por separado. Para el DORA y las categorías digitales abarcadas por el Reglamento 2024/2690, el régimen aplicable se verifica sin asumir la plena aplicación acumulativa de las obligaciones. [R6]

Posibles servicios posteriores

La propuesta se prepara después del alcance y se entiende la necesidad identificada. El pre-audit es una etapa de preparación comercial, no una obligación universal separada. Un cliente puede necesitar proceder directamente a una auditoría o sólo puede necesitar completar ciertas pruebas.

ETAPA	ACTIVIDADES REALIZADAS	RESULTADO CONCRETO
P1 • Evaluación inicial / pre-audita	Aplicabilidad, riesgos, documentos y aplicación; entrevistas y verificaciones autorizadas. Preparación de la autoevaluación según el procedimiento aplicable.	Informe de situación, carencias, evidencias y apoyo a los documentos que deben aprobarse o presentarse.
P2 • Auditoría independiente	Auditoría regulada realizada por un auditor independiente acreditado por DNSC; herramientas, documentos, entrevistas y pruebas dentro del ámbito aprobado.	Informe de auditoría y hallazgos. Un escaneo por sí solo no constituye una auditoría.
P3 • Plan y presupuesto	Prioridades según riesgos, opciones de tratamiento, responsables, plazos, dependencias y costes iniciales/recurrentes.	Plan aprobado y presupuesto transparente; preparación de la presentación cuando sea necesaria.
P4 • Implementación	Soluciones técnicas y organizativas, configuración, formación, pruebas de aceptación y recopilación de evidencias.	Medidas aplicadas y verificadas; limitaciones y riesgos residuales documentados.
P5 • Mantenimiento e información	Revisiones y nuevas pruebas, actualización documental, apoyo a reevaluaciones y comunicaciones pertinentes.	Evidencias e informes de gestión actualizados; apoyo al cierre de medidas.

Contenido necesario de la propuesta

Entre las entidades, sitios y sistemas figuraban servicios y métodos; número de entrevistas y comprobaciones; entregables; límites de acceso; hipótesis; responsabilidades de los clientes; costos iniciales y recurrentes; exclusiones; criterios de aceptación; y condiciones para cambiar el alcance.

Dependiendo del riesgo, un requisito puede ser abordado por configuración, procedimiento, entrenamiento o producto. Elegir una marca no es, por sí mismo, una condición de cumplimiento.

Mantenemos los servicios separados

El cliente no está obligado a comprar cada etapa del mismo proveedor. Implementación y la auditoría independiente tienen roles distintos. Licencias, hardware y operaciones especiales se definen por separado en la propuesta.

Cómo se realiza la verificación técnica

Una herramienta puede ayudar con el inventario y con la comprobación de ciertas configuraciones, permisos, vulnerabilidades o registros, de acuerdo con sus capacidades reales. Por sí misma, no puede demostrar la gobernanza, la aceptación de riesgos, la aplicación de cada procedimiento o el pleno cumplimiento de los requisitos.

Antes de cualquier conexión

ELEMENTO	ACUERDO POR ESCRITO
Alcance y método	Sistemas incluidos/excluidos, método de recogida, escaneos/tests aprobados, ventanas de tiempo y reglas de parada.
Acceso y cambios	Privilegios mínimos; acceso sólo lectura donde el método permite; cuentas controladas revocadas después del trabajo. Cambios requieren aprobación separada.
Datos y confidencialidad	Datos recogidos, almacenamiento, destinatarios, conservación y eliminación. Acuerdos de confidencialidad y tratamiento, cuando proceda.
Terceros y sistemas sensibles	Permiso de propietarios / proveedores; un método seguro y ventanas aprobadas para OT, sistemas médicos y críticos. No escaneo activo por defecto.
Entrega y trazabilidad	Registro de actividad, hallazgos, pruebas pertinentes, limitaciones de herramientas y asuntos que requieren verificación manual.

El cuestionario no autoriza escaneos

Seleccionar “Me gustaría una propuesta” o devolver el libro de Excel no constituye consentimiento para el acceso, la instalación de un agente, el escaneo del sistema o los cambios de configuración.

Quién es responsable y quién verifica

La administración aprueba y supervisa las medidas, proporciona recursos y asume las obligaciones aplicables. El equipo de evaluación y ejecución lleva a cabo el mandato acordado. El auditor acreditado formula independientemente las conclusiones de la auditoría reglamentada. [R1-R2]

La independencia también se verifica cuando el auditor e implementador pertenecen a diferentes empresas del mismo grupo: se examinan los servicios actuales y anteriores, las relaciones profesionales/financieras y las incompatibilidades previstas en el artículo 58. La mera existencia de dos empresas no es suficiente. [R2]

No prometemos la "autorización" de un auditor de la autoevaluación y no presentamos la herramienta como la emisión de la certificación NIS2. Los papeles, las certificaciones y los reconocimientos se verifican en la práctica antes de contraer.

De los hallazgos a la aplicación y el informe

Un plan útil no es una lista de productos. Cada hallazgo debe vincularse a un requisito, una evidencia, el riesgo empresarial y un criterio que demuestre su corrección.

EN EL PLAN	QUÉ DEBE QUEDAR CLARO
Hallazgo y riesgo	Lo que se comprobó, cuál es la brecha, qué actividad puede verse afectada y por qué tiene una prioridad particular.
Opciones y costes	Qué puede resolverse con las soluciones existentes; alternativas; costes iniciales y recurrentes e hipótesis de estimación.
Responsable y plazo	Responsable interno, ejecutor, dependencias, parada necesaria y plazo acordado.
Aceptación y evidencias	Prueba que realizar, evidencia conservada, persona que la acepta y riesgo residual pendiente de tratamiento.
Comunicación	Documento presentado, fundamento y plazo aplicables, aprobación de la dirección y prueba de comunicación a la autoridad.

El calendario se define para cada entidad

La lista de verificación inicial y 05_Plazos marcan los hitos: registro, decisión, evaluación del riesgo, autoevaluación, plan y auditoría. El plazo para la presentación del plan después de la autoevaluación queda separado del plazo de aplicación y de la ruta para el plan de auditoría. Los artículos 12, 18 y 57 de la Ordenanza se revisan por separado. [R2]

El cumplimiento no se limita a presentar un documento. La asistencia para la presentación del plan o la comunicación de la conclusión de las medidas se basa en un mandato, la obligación que se aplica efectivamente y las pruebas. Las medidas incompletas no se declaran completas; los bloqueadores y los plazos revisados se abordan en el marco aplicable.

Los incidentes no esperan al fin del proyecto

El procedimiento operativo debe tener en cuenta la notificación de incidentes importantes: advertencia dentro de las 24 horas y notificación dentro de las 72 horas siguientes a ser consciente, seguido de un informe final y de cualquier actualización dentro de los plazos aplicables, con sujeción a las excepciones legales. [R1-R2]

Qué debe enviarnos ahora

Sólo el libro de trabajo de Excel completado, con la información conocida y las personas/roles que pueden confirmarlo. A continuación, establecimos las aclaraciones, el alcance y la propuesta. Posteriormente se solicitan documentos de apoyo y acceso técnico, a través de un canal seguro y dentro de los límites acordados.

Fundamentos y límites de este documento

El cuestionario técnico CSAT/CISv8 recibido contiene 63 preguntas sobre 20 temas. Se agruparon por temas en 44 preguntas en rumano y se completaron con ámbitos del marco NIS2/DNSC. El registro interno conserva las preguntas originales, su ubicación en Excel y las correspondencias establecidas.

Los niveles básico, estandarizado, racionalizado y dinámico, los valores de riesgo y las recomendaciones comerciales de la fuente no se convirtieron en puntuaciones DNSC, presupuestos ni obligaciones de compra. Un «Sí» es una declaración que debe verificarse, no una prueba. Una respuesta «Posiblemente no aplicable» no establece ni aprueba, por sí sola, una exclusión legal.

Referencias normativas

REF.	FUENTE Y USO
R1	Directiva (UE) 2022/2555: Artículos 20 (gestión), 21 (medidas de gestión de riesgos de seguridad), 23 (incidentes). EUR-Lex: CELEX 32022L2555.
R2	Ordenanza de Urgencia n.º 155/2024, aprobada con modificaciones por la Ley n.º 124/2025, versión consolidada: arts. 11–15, 18, 57–58 y anexos. Portal Legislativo de Rumanía: documento 293121.
R3	Orden del DNSC n.º 1/2026, publicada el 27 de agosto de 2026; anexos sobre medidas y autoevaluación. Portal Legislativo de Rumanía: documentos 314681 / 314360 / 314683.
R4	Orden del DNSC n.º 2/2026: cambios sobre no aplicabilidad y controles de grupo. Portal Legislativo de Rumanía: documento 314676.
R5	Decisión del DNSC n.º 3/2026 y normas para grupos: aplicación, evidencias locales y responsabilidades. Portal Legislativo de Rumanía: documentos 314698 / 314699.
R6	Reglamento (UE) 2022/2554 — DORA y Reglamento de Ejecución (UE) 2024/2690, en sus respectivos ámbitos. EUR-Lex: CELEX 32022R2554 / 32024R2690.

Las direcciones completas y el papel de cada fuente están en la hoja 08_Referencias en Excel. Fecha de referencia del paquete: 6 de octubre de 2026. La legislación y los procedimientos aplicables en la fecha de evaluación de la entidad deben ser utilizados.

Términos, en breve

MFA: autenticación mediante más de un factor. OT: sistemas que controlan procesos físicos o equipos. Copia de seguridad: su existencia no demuestra una restauración satisfactoria. Evidencia: documento, registro o resultado de una prueba que respalda un hallazgo. Riesgo residual: riesgo que permanece después de aplicar las medidas.

Coordinación de la solicitud

Cristian Apostol • office@clarified.ro • +40 774 456 127
it.clarified.ro/nis2