ITINERARIO AVANZADO · MONOGRÁFICO 3

NIS2 y NIST CSF 2.0

Seguridad de los sistemas de IA

Gobierno, riesgos, protección, proveedores, detección, respuesta y recuperación.

Conexión con el SGIA e ISO/IEC 42001

José Manuel Hernández Agudo

Cuaderno de estudio y práctica · 25 de octubre de 2026

Ocho lecciones desarrolladas · Herramientas H01-H08 · Casos y actividades resueltas · Infografías · Espacios de trabajo

Cómo utilizar este cuaderno

Lee cada lección y trabaja sus actividades antes de consultar la orientación resuelta. Las fichas y los modelos permiten aplicar el método a un alcance concreto. Los ejemplos de Tech Server IIT Spain son ficticios; los supuestos adicionales se identifican expresamente.

Puedes escribir en los campos interactivos o imprimir las páginas de práctica. Guarda una copia propia y comprueba que tus respuestas se conservan al volver a abrirla. No introduzcas datos personales innecesarios, secretos ni credenciales reales.

Campos e impresión

Un campo puede conservar más texto del que muestra su caja. Ese contenido desplazado puede quedar fuera de la impresión. Si tu respuesta supera el espacio visible, utiliza las hojas de ampliación al final e indica la lección o herramienta a la que corresponde. Revisa siempre la vista de impresión.

Un expediente que se pueda reconstruir

Diferencia hechos, hipótesis, propuestas y decisiones. Identifica fuentes, alcance, responsables y pendientes. No completes una autorización o un resultado de prueba por parecer razonable. Las correspondencias normativas sirven para coordinar trabajo y evidencias; cada obligación conserva su propio fundamento.

Navegación

El índice y los marcadores del lector PDF permiten ir a cada sección. Las referencias oficiales son enlaces. Las herramientas CSV y los modelos del ZIP complementan los campos del cuaderno. Las tres clases están publicadas en iVoox y enlazadas en las lecciones 3, 5 y 8. Sus aclaraciones escritas acompañan cada clase. Los datos de publicación y las notas también están en Audios.

Índice de estudio y práctica

Cómo utilizar este cuaderno 2

NIS2 y NIST CSF 2.0: seguridad de los sistemas de IA 4

Lección 1. Delimitar el ámbito y entender las responsabilidades 6

Lección 2. Gobernar el riesgo y fijar prioridades 15

Lección 3. Identificar activos, dependencias y escenarios 21

Lección 4. Proteger datos, identidades y configuraciones 27

Lección 5. Gestionar proveedores y cadena de suministro 32

Lección 6. Detectar señales y comprobar la vigilancia 38

Lección 7. Responder, investigar y decidir las comunicaciones 44

Lección 8. Recuperar el servicio y comprobar la mejora 50

Alcance y aplicabilidad 56

Responsabilidades y formación para gobernar la seguridad de la IA 58

Perfil y prioridades 63

Activos, dependencias y escenarios 65

Protección y pruebas 67

Evaluación rápida de proveedores y componentes de IA 69

Detección y cobertura 74

Formularios de clasificación y comunicaciones 76

Evaluar y notificar un incidente significativo 79

Recuperación y eficacia 84

Tres ejemplos para trabajar gobierno, notificación y proveedores 94

Caso final. Presentar un expediente de seguridad de IA a dirección 99

Matriz funcional: NIS2, NIST CSF 2.0 y SGIA 102

Glosario y códigos para navegar por el monográfico 105

Fuentes oficiales y cómo utilizarlas 107

NIS2 y NIST CSF 2.0: seguridad de los sistemas de IA

Monográfico 3 del itinerario avanzado · Fundamentos del SGIA e ISO/IEC 42001

José Manuel Hernández Agudo · 25/10/2026

Qué construirás

Un expediente que permita explicar qué servicio y sistemas protegemos, quién decide, qué controles funcionan y cómo se actúa, comunica y recupera ante un problema. NIS2 aporta el marco jurídico que se analiza para la entidad; NIST CSF 2.0 organiza resultados de ciberseguridad; el SGIA conecta finalidad, responsabilidades, riesgos, impactos, evidencia y decisiones.

Cómo estudiar

Lee cada lección y completa su herramienta. Intenta las actividades antes de consultar la orientación resuelta. Distingue qué está acreditado, qué se propone y qué sigue pendiente. Utiliza las infografías para recorrer las decisiones y el PDF para estudio y práctica. Conserva tus respuestas en una carpeta propia.

La carga orientativa es de unas doce a quince horas, incluyendo las ocho sesiones, herramientas y caso final; depende de experiencia y profundidad del expediente. Es una propuesta pedagógica, no una carga reglamentaria.

Sesión	Contenido	Trabajo de salida
1	Ámbito y responsabilidades	H01, RACI y necesidades de formación
2	Riesgo y prioridades	H02, perfil y plan de brechas
3	Activos y escenarios	H03, dependencias y comprobaciones
4	Protección	H04, criterios y pruebas
5	Proveedores	H05, veinte preguntas y propuesta de decisión
6	Detección	H06, prueba por etapas y límites
7	Respuesta y comunicaciones	H07, significatividad, cronología y formularios
8	Recuperación y eficacia	H08 y expediente final a dirección

Caso y supuestos

Tech Server IIT Spain es ficticia. SYS-003 / USO-004 conserva v1 90/100 global y 9/10 críticos; v2 94/100 y 7/10. v2 está probada, sin autorización de despliegue. No se autoriza v1 por comparación ni se atribuye un ataque a las métricas. T10-014 conserva sus incógnitas. Los supuestos C3-ALC-01, C3-GOB-01, C3-DEP-01, C3-PRO-01, C3-SUP-01, C3-DET-01, C3-NOT-01 y C3-REC-01 se identifican expresamente y no modifican esos hechos.

Integración con ISO/IEC 42001

El trabajo se relaciona con gobierno, competencia, riesgos, impactos, operación, evaluación y mejora del SGIA. Las áreas del anexo A ayudan a ordenar conexiones: A.3 organización; A.4 recursos; A.5 impactos; A.6 ciclo de vida; A.7 datos; A.8 información para partes interesadas; A.9 uso; A.10 terceros y clientes. Las herramientas plantean relaciones funcionales y selección justificada de controles, sin declarar equivalencias completas entre normas.

Audios y materiales de apoyo

Las tres clases están publicadas en iVoox según los enlaces facilitados por el autor. Se escuchan al finalizar cada bloque; las aclaraciones escritas acompañan la clase en la lección correspondiente.

- 045. NIS2 y NIST CSF 2.0: gobierno de IA y responsabilidad directiva. Al terminar la lección 3.
- 046. NIS2 y NIST CSF 2.0: protección y proveedores de IA. Al terminar la lección 5.
- 047. NIS2 y NIST CSF 2.0: detección, notificación y recuperación. Al terminar la lección 8.

El ZIP incluye las notas de aplicación y los datos de publicación en Audios. Las fuentes y prompts vigentes se conservan en NotebookLM como apoyo documental; no necesitas generar nuevas grabaciones.

Los trece módulos principales mantienen su estructura. Este monográfico tiene su propia numeración dentro de los seis módulos avanzados. Los proyectos de InditexTech corresponden a la fase posterior.

Lección 1. Delimitar el ámbito y entender las responsabilidades

Monográfico 3 · NIS2 y NIST CSF 2.0: seguridad de los sistemas de IA

José Manuel Hernández Agudo · 25/10/2026

Qué aprenderás

- Diferenciar entidad, servicio, sistema y uso de IA para definir qué se protege.
- Investigar la aplicabilidad de NIS2 sin deducirla del nombre de la empresa o del uso de IA.
- Entender qué aporta el CSF 2.0 y cómo se conecta con el SGIA.
- Organizar una decisión inicial con hechos, fuentes, responsabilidades y evidencias.
- Asignar tareas y autoridad mediante una RACI y preparar la formación de quienes gobiernan la seguridad y la IA.

Resultado esperado: una ficha de alcance con su matriz de responsabilidades y necesidades de formación, que permita explicar qué se sabe, qué debe comprobarse y qué actuación puede comenzar mientras se completa el análisis.

Una mejora del promedio no explica un problema de seguridad

En el caso de Tech Server IIT Spain, la v2 del clasificador SYS-003 mejora su exactitud global y detecta menos tickets críticos que v1. Ya sabemos describir esos resultados. Al empezar a estudiar ciberseguridad surge otra pregunta: ¿la diferencia demuestra que alguien haya manipulado los datos o atacado el sistema?

Los porcentajes no permiten llegar a esa conclusión. Tampoco descartan un problema de seguridad. Para investigar necesitamos identificar configuración, datos, protocolo y evidencias pertinentes. Un escenario de ataque puede orientar una comprobación, pero sigue siendo una hipótesis hasta que los hechos lo sostengan.

La v2 conserva su estado: **probada, sin autorización de despliegue**. Esta lección no la sitúa en producción. Las decisiones operativas del servicio deben referirse a la versión y al uso efectivamente autorizados, que habrá que comprobar en los registros.

Este será el criterio del monográfico: relacionar riesgos, medidas, comprobaciones y decisiones con un alcance que podamos describir.

1. Empezar por el servicio que queremos proteger

La seguridad de una IA depende también del servicio que la utiliza y de su cadena técnica. Si solo examinamos el modelo, podemos dejar fuera cuentas con permisos excesivos, un repositorio, un servicio contratado, una interfaz o los registros necesarios para detectar un uso indebido.

Para trabajar ordenadamente distinguiremos cuatro planos:

Plano	Pregunta de trabajo	Aplicación al curso
Entidad	¿Qué organización realiza la actividad y asume las responsabilidades?	Tech Server IIT Spain, empresa ficticia. Su situación jurídica se debe justificar.
Servicio	¿Qué prestación o actividad queremos mantener y qué consecuencias tendría su alteración?	La actividad de soporte a la que contribuye el clasificador, con límites y dependencias por confirmar.

Plano	Pregunta de trabajo	Aplicación al curso
Sistema	¿Qué componentes intervienen y en qué versión o entorno?	SYS-003, incluyendo las dependencias que se identifiquen mediante evidencias.
Uso de IA	¿Para qué se utiliza la salida y qué decisión o actuación viene después?	USO-004, conservando su finalidad y la supervisión que se documenten.

No necesitamos dibujar toda la empresa antes de actuar. Sí necesitamos un alcance suficiente para que otra persona comprenda qué estamos evaluando y qué queda fuera.

Una ficha inicial útil identifica también propietario del servicio, funciones de revisión y decisión, proveedores relevantes y registros que se consultarán. Si un dato falta, se asigna su comprobación: el pendiente debe tener una pregunta concreta y un siguiente paso.

2. Qué hay que investigar antes de afirmar que NIS2 nos afecta

NIS2 es la Directiva (UE) 2022/2555. Su ámbito se analiza considerando los tipos de entidades y sectores, las reglas de tamaño y los supuestos específicos previstos en su articulado. La clasificación entre entidad esencial e importante tiene sus propias reglas. Utilizar IA o llamar «crítico» a un ticket no resuelve ese análisis. [F1]

En una organización de servicios TI, la investigación puede incluir si su actividad encaja en la gestión de servicios TIC entre empresas y qué servicio presta efectivamente. Tener un departamento de informática interno no demuestra por sí solo que la entidad sea un proveedor de servicios gestionados comprendido en esa categoría.

La ficha deberá responder, al menos:

1. Qué actividad realiza la entidad y bajo qué organización jurídica.
2. Qué categoría y sector se están examinando y con qué fundamento.
3. Qué datos de tamaño y relaciones empresariales deben considerarse, y si existen reglas específicas aplicables.
4. Qué jurisdicción y disposiciones nacionales corresponden al servicio y a la entidad.
5. Qué conclusión puede sostenerse y qué comprobación falta para resolver el resto.

También se revisan las obligaciones contractuales y otras normas que puedan afectar a la prestación. Una empresa puede recibir exigencias de seguridad de un cliente aunque todavía no haya establecido que queda directamente comprendida en NIS2. Cada obligación debe conservar su fuente: una cláusula contractual no se presenta como un artículo de la Directiva.

3. Distinguir el marco europeo y su aplicación en España

Para una entidad situada en España debemos separar el contenido de la Directiva, las normas nacionales aplicables y las disposiciones europeas que puedan resultar pertinentes al servicio. Este trabajo no se resuelve leyendo únicamente un resumen del anteproyecto de una ley.

Como hito documental, la Comisión Europea comunicó el **8 de julio de 2026** su decisión de llevar a España y otros Estados ante el Tribunal de Justicia por no notificar las medidas de transposición de NIS2. Esa comunicación identifica una situación en una fecha concreta; la conclusión sobre una organización necesita las fuentes y disposiciones que correspondan a su expediente. [F6]

Por tanto, en la ficha se registran la norma consultada, la edición o versión, la fecha y el razonamiento de aplicabilidad. No se convierte una propuesta legislativa en una obligación ya vigente, ni se concluye que el servicio carezca de deberes de seguridad por existir un problema de transposición.

Cuando la actividad esté comprendida en su ámbito, deberá examinarse asimismo el Reglamento de Ejecución (UE) 2024/2690. La guía de ENISA de 2025 ayuda a interpretar sus medidas técnicas y metodológicas para las entidades a las que se dirige. Es una guía con recomendaciones y ejemplos de evidencia; su alcance se comprueba antes de trasladar una recomendación como obligación general. [F5, F7]

4. Qué aporta NIST CSF 2.0

El CSF permite organizar resultados de ciberseguridad y conversar sobre ellos entre dirección, equipos técnicos y terceros. No fija una receta idéntica para todas las organizaciones: las actuaciones se concretan según contexto, riesgo y requisitos. [F2, F3]

Sus seis funciones ayudan a formular preguntas:

Función	Pregunta para nuestro expediente
Gobernar	¿Quién decide las prioridades, responsabilidades y límites de riesgo?
Identificar	¿Qué activos, dependencias y riesgos afectan al servicio?
Proteger	¿Qué medidas reducen la exposición y sostienen el servicio?
Detectar	¿Qué señales buscamos y cómo comprobamos su cobertura?
Responder	¿Cómo actuamos y coordinamos una investigación o comunicación?
Recuperar	¿Qué permite restablecer el servicio y comprobar su funcionamiento?

Estas funciones se relacionan durante toda la gestión; el orden de lectura no obliga a ejecutar un ciclo lineal ni a terminar una función antes de atender otra.

El **perfil actual** describe la situación respecto de los resultados examinados. El **perfil objetivo** identifica los resultados que la organización pretende alcanzar y priorizar. En la lección 2 utilizaremos esa diferencia para organizar un plan de mejora con evidencias, responsables y seguimiento. [F8]

Un informe de un tercero sobre CSF puede aportar información útil si conocemos su alcance y método. NIST no ofrece certificaciones o avales de productos, implementaciones o servicios relacionados con el CSF. Una afirmación comercial de «certificado NIST» requiere aclarar quién evaluó qué y con qué criterio; no demuestra por sí sola cumplimiento de NIS2. [F4]

5. Cómo llevarlo al SGIA

El SGIA conecta la seguridad con la finalidad del sistema, las personas afectadas y las decisiones de la organización. Para ello reutilizaremos sus procesos y registros cuando sean pertinentes:

- **R-001 e IMP-001:** vincular escenarios de seguridad con riesgos e impactos, conservando el contexto del uso de IA.
- **FD-001 y registros de datos:** identificar fuentes, accesos, versiones y protección cuando correspondan al sistema examinado.
- **PROV-001 y CAM-001:** relacionar dependencias, cambios, pruebas y autorización.
- **MON-001 e INC-001:** conservar señales, investigación, medidas y decisiones de comunicación.
- **Gobierno, competencia, auditoría y revisión:** definir autoridad, medios y comprobación de eficacia.

No se crean nuevas autorizaciones copiando un estado a otra ficha. Para SYS-003 / USO-004 / v2 se conserva «probada, sin autorización de despliegue» y se identifica la fuente autorizada del dato. La conexión propuesta en este monográfico es funcional: sirve para coordinar el trabajo y sus evidencias.

5.1. Quién aprueba y quién realiza el trabajo

El artículo 20 de NIS2 sitúa en los órganos de dirección de las entidades esenciales e importantes la aprobación y supervisión de las medidas de gestión de riesgos del artículo 21 y la responsabilidad prevista en ese marco. Debe identificarse qué órgano corresponde a la estructura de la entidad y cómo se concreta el régimen aplicable. Designar un AI Officer -AIO- o un CISO no sustituye esas responsabilidades. Esas denominaciones se utilizan aquí para organizar funciones internas; el artículo 20 no impone cargos con esos nombres.

En nuestra propuesta, el AIO conecta finalidad, riesgos e impactos, supervisión y autorizaciones de IA. El CISO coordina seguridad, detección, respuesta y recuperación. Operación aporta los hechos y realiza las actuaciones del servicio. Dirección decide dentro de sus competencias y delegaciones; el órgano correspondiente aprueba y supervisa las medidas que le incumben.

La herramienta **C3-H01A, Responsabilidades y formación directiva**, desarrolla una matriz RACI de dieciséis tareas. Identifica quién realiza, quién decide internamente, quién es consultado y quién recibe información. La asignación se completa con titulares, suplentes y límites de autoridad. Su aprobación no convierte una propuesta de despliegue en un despliegue autorizado.

5.2. Qué formación necesita quien decide

El artículo 20.2 prevé asistencia a formación de los miembros de los órganos de dirección para identificar riesgos y evaluar la gestión de ciberseguridad y su repercusión en los servicios. La formación en IA se fundamenta por separado: se identifican las medidas de alfabetización del artículo 4 del AI Act que correspondan a la organización y las competencias necesarias para cada función del SGIA.

En su redacción modificada en 2026, el artículo 4 exige medidas de apoyo a la alfabetización atendiendo al contexto del personal y de quienes operan o utilizan sistemas por cuenta de proveedores o responsables del despliegue. No exige garantizar un nivel específico de alfabetización de cada persona. No equivale a un certificado universal obligatorio para cada consejero. [F9]

La herramienta propone cinco horas de formación y ejercicio para quienes gobiernan estas decisiones: dos de ciberseguridad, dos de IA y una de simulación de incidente. Es una propuesta interna, no un mínimo legal. Se conserva evidencia de asistencia y del resultado de ejercicios pertinentes; una firma de asistencia no demuestra por sí sola capacidad para decidir.

Trabajo de aplicación: completa C3-H01A para el alcance de tu ficha. Identifica quién puede activar una medida urgente, quién puede comunicar y qué ocurre si el titular no está disponible. Las actividades y ejemplos de la herramienta permiten comprobar la asignación sin inventar nombramientos de Tech Server IIT Spain.

6. Caso guiado: una regla de acceso que se pueda comprobar

Supuesto didáctico adicional C3-ALC-01. Los datos siguientes se introducen únicamente para este ejercicio. No describen controles ya implantados ni incidentes reales de Tech Server IIT Spain.

El equipo prepara un entorno de evaluación del clasificador. Su inventario de ejercicio muestra dos cuentas con permisos administrativos. Una tiene responsable identificado; la otra utiliza una denominación compartida y carece de responsable registrado. No se aporta evidencia de uso indebido, conexión con producción ni daño.

La propuesta de calidad y seguridad es que cada acceso administrativo incluido en el alcance tenga una responsabilidad y una justificación verificables. Es un criterio interno de trabajo del supuesto; todavía no se atribuye a una obligación legal concreta.

Trabajo resuelto

Elemento	Respuesta del modelo
Alcance	Los dos accesos administrativos del entorno de evaluación definido en el supuesto.
Hecho observado	Uno tiene responsable registrado y el otro no.
Conclusión que se puede sostener	La atribución de responsabilidad está incompleta en la muestra examinada.
Conclusión que no está acreditada	Que haya existido un acceso ilícito o que la cuenta sin responsable haya causado un incidente.
Resultado deseado	Identificar la responsabilidad y la necesidad de cada acceso, con una revisión y una decisión documentadas.
Actuación propuesta	Confirmar quién utiliza la cuenta compartida, sus permisos y dependencias; valorar la medida adecuada y comprobar el resultado antes de dar el control por resuelto.
Evidencia de comprobación	Inventario actualizado, revisión de permisos, fundamento de la decisión y prueba de que se conserva el acceso necesario y se retira el que corresponda.
Conexión con el SGIA	Riesgos, recursos, control de cambios y evidencia de la decisión, utilizando los registros pertinentes.

Eliminar una cuenta sin analizar sus dependencias podría interrumpir una prueba o una operación legítima. Mantenerla sin investigar tampoco resuelve la falta de responsabilidad. La propuesta debe permitir decidir con información y comprobar el efecto de la medida.

El caso muestra cómo una expectativa general se convierte en una comprobación concreta. Esa es la utilidad de trabajar conjuntamente alcance, gobierno, protección y evidencias.

Actividad 1. Corregir una afirmación de cumplimiento

Enunciado hipotético: «El proveedor nos ha enviado un certificado NIST y nuestro SGIA dispone de procedimientos. Podemos marcar NIS2 como cumplido».

Redacta una respuesta profesional y explica qué comprobarías antes de cerrar la conclusión.

Orientación resuelta

Qué. Sustituir la afirmación general por una revisión de aplicabilidad, alcance y evidencia. Una respuesta posible es: «Revisaremos qué obligaciones corresponden a la entidad y al servicio, qué evaluación aporta el proveedor y qué resultados propios están comprobados antes de formular una conclusión».

Por qué. Un procedimiento escrito no demuestra su ejecución. Un documento de un tercero puede tener un alcance limitado. El uso del CSF no crea una declaración automática de conformidad con NIS2.

Cómo. Identificar entidad, servicio y sistemas; documentar las fuentes aplicables; comprobar emisor, objeto y método del informe recibido; relacionar sus evidencias con las de la integración; registrar las brechas y las decisiones necesarias.

Cuándo. Antes de utilizar esa conclusión para aceptar un cambio, responder a un cliente o comunicar cumplimiento.

Dónde. En la ficha de alcance y aplicabilidad, enlazada al expediente del sistema, los contratos y los registros del SGIA.

Con qué. Fuentes oficiales, condiciones contractuales, documentación del proveedor, resultados de pruebas y personas competentes para la revisión. Se conserva la distinción entre lo documentado, lo comprobado y lo

pendiente.

Actividad 2. Interpretar la caída en críticos

Enunciado: alguien afirma que pasar de 9/10 a 7/10 críticos detectados demuestra que el clasificador sufrió un ataque y que v2 debe figurar como sistema implicado en T10-014.

Explica qué permite concluir la información del caso y prepara la siguiente actuación.

Orientación resuelta

Qué. Registrar la diferencia informada y organizar las comprobaciones pertinentes sin atribuir un ataque ni una causa a T10-014.

Por qué. Un resultado agregado describe una muestra; no establece su causa ni identifica por sí solo una versión implicada en otro episodio. La falta de autorización de despliegue de v2 tampoco demuestra imposibilidad técnica de intervención.

Cómo. Conservar los informes; identificar configuración, protocolo, datos y registros; verificar la comparabilidad y las posibles explicaciones; separar hechos e hipótesis. Si se investiga T10-014, comprobar su cronología y versión efectiva y analizar las obligaciones pertinentes desde el inicio.

Cuándo. Al detectar la diferencia y antes de emitir una conclusión causal o una comunicación que la dé por acreditada.

Dónde. En los registros de pruebas y riesgos que correspondan; y en el expediente de T10-014 únicamente cuando exista una relación sustentada o una hipótesis de investigación expresamente identificada.

Con qué. Informes originales, datos de evaluación, configuración, trazas y revisión competente. La v2 conserva «probada, sin autorización de despliegue» y v1 no se autoriza por comparación.

Comprueba lo aprendido

1. ¿Usar IA basta para afirmar que una organización está comprendida en NIS2? No. La aplicabilidad se investiga con las reglas y fuentes pertinentes.
2. ¿Una categoría interna de ticket crítico determina la clasificación jurídica de la entidad o del sistema? No.
3. ¿El CSF ofrece la misma lista de actuaciones obligatorias para todas las organizaciones? No. Ayuda a organizar y priorizar resultados según el contexto.
4. ¿Las seis funciones deben ejecutarse una después de otra y quedar terminadas? No. Se mantienen relacionadas durante la gestión.
5. ¿Una cuenta sin responsable registrado prueba un ataque? No. Es una carencia concreta que necesita investigación y tratamiento.
6. ¿Se puede calificar T10-014 automáticamente como incidente significativo de NIS2 o grave del AI Act? No. Cada categoría exige su propio análisis de aplicabilidad y hechos.

Evidencia de salida

Prepara una ficha con entidad, servicio, sistema y uso, versiones y entornos incluidos, fuentes legales y contractuales, conclusión razonada de aplicabilidad, funciones de revisión y decisión y próximas comprobaciones. Añade una medida propuesta y explica qué evidencia permitiría comprobar su resultado. Adjunta la RACI C3-H01A, sus suplencias y las necesidades de formación identificadas, distinguiendo obligaciones legales y requisitos internos.

La ficha será útil si otra persona puede reconstruir el alcance, identificar el fundamento de cada afirmación y saber quién debe actuar después.

Fuentes

F1. Directiva (UE) 2022/2555: texto oficial, especialmente ámbito, gobernanza y medidas de gestión de riesgos.

F2. NIST CSF 2.0: publicación oficial.

F3. NIST SP 1299: guía de recursos y descripción general en español.

F4. NIST: preguntas frecuentes sobre uso, resultados y certificación del CSF.

F5. ENISA: guía técnica de implementación de NIS2, 2025.

F6. Comisión Europea: decisión de remisión al TJUE, 8 de julio de 2026.

F7. Reglamento de Ejecución (UE) 2024/2690.

F8. NIST SP 1301: creación y utilización de perfiles organizativos.

F9. Reglamento (UE) 2026/1744, artículo 1.5: modificación del artículo 4 del AI Act.

CURSO SGIA · MONOGRÁFICO 3

Delimitar y asignar responsabilidades

NIS2 + NIST CSF 2.0 · Lección 1

01 Entidad, servicio, sistema y uso

Describe qué se protege y dónde termina el alcance. La actividad y los hechos sostienen el análisis.

02 Aplicabilidad con fuentes y hechos

Usar IA o llamar crítico a un ticket no resuelve el ámbito jurídico de NIS2.

03 Aprobación y supervisión de dirección

La dirección necesita medidas aprobadas, información de ejecución y seguimiento de carencias.

04 AIO, CISO, operación y suplencias

Asigna tareas, autoridad y suplentes. La formación en IA y ciberseguridad conserva su fundamento.

TU EVIDENCIA DE SALIDA

H01 + RACI: alcance, autoridad y formación

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 1. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 2. Gobernar el riesgo y fijar prioridades

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Convertir riesgos del servicio en decisiones, recursos y comprobaciones; construir un perfil actual y un perfil objetivo; explicar por qué una brecha tiene prioridad. Trabajo orientativo: 90 minutos entre estudio y aplicación, adaptable a la experiencia del alumno.

1. La dirección necesita decisiones que pueda supervisar

Un informe de seguridad puede contener muchas vulnerabilidades y aun así no explicar qué debe decidir la dirección. Para que sea útil debe relacionar el problema con el servicio, sus consecuencias, las opciones y la autoridad necesaria. «Hay que mejorar los accesos» describe una intención. «No se conoce quién utiliza una cuenta administrativa del entorno de evaluación; necesitamos comprobar su necesidad y permisos y decidir el tratamiento antes de ampliar el acceso» permite asignar una actuación y verificar su cierre.

NIS2 sitúa la aprobación y supervisión de medidas en el gobierno de las entidades comprendidas en su ámbito. La gestión no termina cuando se aprueba una política: hace falta información sobre ejecución, carencias y resultados. El SGIA permite conectar esas decisiones con finalidad, riesgos, impactos y autorizaciones de IA. La RACI de la lección 1 aclara quién prepara información, ejecuta y decide. [F1]

El CISO puede recomendar una medida, el AIO explicar su efecto sobre la supervisión de IA y operación señalar una dependencia que impida aplicarla inmediatamente. La dirección necesita reconocer esas interacciones. Suspender un acceso podría reducir exposición y también interrumpir una tarea legítima; mantenerlo sin revisar preservaría esa tarea, pero dejaría el riesgo sin tratamiento suficiente. La decisión debe describir qué alternativa se elige, con qué límites y cómo se comprueba.

2. Describir un riesgo antes de puntuarlo

Una descripción útil enlaza activo o dependencia, condición, evento y consecuencia. Ejemplo adicional: «Una cuenta compartida sin atribución suficiente podría permitir modificaciones que no podamos vincular a una persona; eso dificultaría investigar alteraciones de pruebas y sostener decisiones sobre el clasificador». La existencia de la cuenta no prueba que ya se haya producido esa modificación.

Elemento	Pregunta que ayuda a precisarlo
Servicio y alcance	¿Dónde importa este riesgo y qué entorno se ha examinado?
Condición	¿Qué hecho o carencia sostiene el escenario?
Evento	¿Qué podría ocurrir, accidentalmente o por una actuación indebida?
Consecuencia	¿Qué afectaría a operación, personas, información o decisiones?
Medidas existentes	¿Qué reduce la exposición y qué evidencia tenemos de su funcionamiento?
Incertidumbre	¿Qué dato falta y cómo podría cambiar la decisión?

La evaluación puede ser cualitativa o cuantitativa si el método y los datos lo permiten. Multiplicar números asignados sin fundamento no convierte una opinión en una medida precisa. Las escalas internas deben explicar qué significan sus categorías y cómo se utilizan. La prioridad de una obligación con plazo no se

decide únicamente por una puntuación de riesgo.

3. Perfil actual y perfil objetivo del CSF

El perfil actual identifica los resultados de ciberseguridad que se están logrando en un alcance. El perfil objetivo expresa los resultados que se pretende alcanzar atendiendo al contexto. Compararlos ayuda a organizar brechas y acciones. No hay un perfil único que sirva como certificado para cualquier entidad. Las funciones del CSF se mantienen relacionadas: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. [F2, F3]

En H02 utilizaremos cuatro conclusiones de trabajo: **acreditado en el alcance examinado**, **parcial**, **no evidenciado** y **no revisado**. Son estados internos de esta herramienta, no niveles oficiales del CSF. «No evidenciado» evita afirmar que un control no existe cuando lo que falta es soporte suficiente. «No revisado» conserva el límite del trabajo realizado.

El perfil objetivo debe describir un resultado observable. «Comprar una plataforma» es una acción. «Poder detectar y escalar una pérdida de registros del servicio dentro del objetivo interno definido» describe un resultado que puede admitir varias soluciones.

Supuesto adicional C3-GOB-01

Se propone un plan para el entorno de evaluación del supuesto C3-ALC-01. No se afirma que estas medidas estén implantadas en Tech Server IIT Spain.

Resultado deseado	Situación conocida del supuesto	Prioridad propuesta y fundamento	Evidencia de salida
Atribuir y justificar los accesos administrativos	Una de dos cuentas carece de responsable registrado	Primera: afecta a la atribución y a decisiones posteriores	Revisión de cuentas, dependencias y permisos; decisión y comprobación
Reconstruir la configuración utilizada en una prueba	No se ha aportado el expediente suficiente	Primera: sin ello no se puede sostener la comparación de resultados	Identificación de versiones, datos y protocolo de prueba
Conocer si la vigilancia deja de recibir registros	No revisado	Comprobar antes de afirmar cobertura	Ensayo controlado de pérdida de recepción y escalado
Recuperar un entorno sin alterar evidencia necesaria	No revisado	Evaluar dependencia y efecto antes de planificar el ensayo	Plan y prueba de recuperación vinculados a los objetivos del servicio

Las prioridades son una propuesta docente basada en esas carencias. No constituyen un diagnóstico global de la empresa. Para llevarlas a operación habría que confirmar el alcance, las medidas existentes y las dependencias.

4. De la brecha al compromiso de trabajo

Cada brecha necesita una acción con responsable, medios, fecha o hito y criterio de cierre. «Enviar un correo al proveedor» puede ser un paso, pero no siempre resuelve la brecha. El cierre debe referirse al resultado: condiciones suficientes obtenidas y revisadas, configuración comprobada o prueba repetida con resultado pertinente.

También se documentan riesgos residuales y condiciones temporales. Una aceptación de riesgo debe provenir de quien tenga autoridad y respetar las obligaciones aplicables; no convierte un incumplimiento legal en permitido. Si la organización limita provisionalmente un uso, registra el alcance y el seguimiento. La palabra «temporal» sin revisión ni responsable no limita por sí sola el riesgo.

La dirección recibe un resumen con decisiones solicitadas, medidas en curso, evidencias suficientes, carencias y cambios relevantes. Las acciones vencidas no desaparecen del informe porque alguien haya modificado su fecha: se conserva historial y motivo del cambio. El SGIA debe permitir reconstruir quién decidió qué y con qué información.

5. Cómo interpretar los niveles del CSF

Los cuatro niveles -Partial, Risk Informed, Repeatable y Adaptive, según la denominación de NIST- ayudan a caracterizar el rigor del gobierno y la gestión del riesgo. No son una escala universal de certificación ni un objetivo obligatorio de llegar siempre al nivel más alto. Deben interpretarse con su alcance y contexto. [F4]

En este curso no calcularemos un nivel promediando casillas de las herramientas. Una organización puede tener prácticas formales y fallos de ejecución; otra, buenos resultados en un ensayo y una gestión poco repetible. El perfil permite describir resultados; el análisis de las prácticas ayuda a entender cómo se sostienen. Ambos necesitan evidencias.

Actividad 1. Priorizar sin inventar precisión

Enunciado: se propone asignar prioridad baja a la cuenta sin responsable porque «solo es un laboratorio» y prioridad alta a comprar una nueva plataforma sin explicar qué resultado mejorará.

Qué. Preparar una priorización basada en el alcance y las consecuencias del servicio, con una comprobación concreta para cada propuesta.

Por qué. Un entorno de evaluación puede contener datos o decisiones relevantes; comprar una herramienta no demuestra que el riesgo se haya tratado.

Cómo. Confirmar datos y accesos del laboratorio, describir el escenario, revisar medidas existentes y comparar alternativas. Para la plataforma, definir primero el resultado necesario y cómo se comprobará.

Cuándo. Antes de aprobar recursos o cerrar la revisión del riesgo.

Dónde. En H02, enlazado a R-001, la ficha de alcance y la RACI.

Con qué. Inventario, revisión de permisos, responsables del servicio y criterios internos de riesgo documentados.

Actividad 2. Una puntuación verde no autoriza el despliegue

Enunciado: un tablero muestra un promedio favorable de medidas. Se propone marcar SYS-003 v2 como autorizada, aunque el expediente mantiene su estado previo.

Qué. Conservar **probada, sin autorización de despliegue** y separar el tablero de seguridad de la decisión de autorización.

Por qué. Un promedio puede ocultar una carencia decisiva. La autoridad sobre el estado se identifica en el expediente, no en el color del panel.

Cómo. Revisar criterios de cambio, resultados pertinentes, riesgos e impactos, supervisión y autoridad. Elevar la decisión con carencias explícitas; no crear una autorización copiando un estado.

Cuándo. Antes de cualquier cambio de entorno o uso.

Dónde. En CAM-001 y en la fuente autorizada del estado, con referencias desde H02.

Con qué. Expediente de pruebas y cambio, decisiones identificadas y evidencias de los controles que correspondan.

Comprueba lo aprendido

1. ¿Un perfil objetivo es una lista de productos? No: describe resultados que se quieren alcanzar.
2. ¿No revisado significa que el control no existe? No: señala un límite de la evaluación.

3. ¿Una aceptación interna permite incumplir una obligación legal? No.
4. ¿El nivel más alto del CSF es obligatorio para toda entidad? No.

Evidencia de salida

Completa H02 con al menos tres resultados, situación actual y soporte, objetivo, brecha, prioridad justificada, actuación, responsable y criterio de cierre. Una segunda persona debe poder explicar por qué esas prioridades son razonables para el alcance examinado.

Fuentes

F1. NIS2, artículos 20 y 21.

F2. NIST CSF 2.0.

F3. NIST SP 1301: perfiles organizativos.

F4. NIST SP 1302: niveles del CSF.

CURSO SGIA · MONOGRÁFICO 3

Gobernar el riesgo y fijar prioridades

NIS2 + NIST CSF 2.0 · Lección 2

01 Describir condición, evento y consecuencia

Un riesgo debe explicar qué podría pasar y a qué servicio o personas afectaría.

02 Separar evidencia actual y objetivo

Distingue acreditado, parcial, no evidenciado y no revisado, sin inventar resultados.

03 Priorizar con fundamento y recursos

El objetivo describe un resultado. La compra de una herramienta es una posible actuación.

04 Cerrar con comprobación del resultado

Define responsable, medios y criterio de cierre. Un promedio verde no crea autorización.

TU EVIDENCIA DE SALIDA

H02: perfil, brechas y decisiones trazables

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 2. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 3. Identificar activos, dependencias y escenarios

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Construir un mapa útil para proteger un servicio de IA; separar amenazas, vulnerabilidades, fallos e incidentes; vincular escenarios a riesgos e impactos sin convertir una hipótesis en un hecho. Trabajo orientativo: 90 minutos.

1. El modelo no es todo el sistema

Un servicio puede depender de datos, componentes, identidades, infraestructura, personas y terceros. El modelo puede funcionar como se esperaba y el servicio fallar porque una credencial caducó, se perdió una cola de trabajo o la persona que debía revisar una salida no recibió el aviso. Examinar solo la exactitud del modelo deja fuera esas dependencias.

El mapa empieza en la finalidad y recorre qué información entra, qué transformación o decisión se realiza y quién utiliza la salida. Después identifica los componentes que hacen posible ese recorrido. No exige dibujar cada cable: exige el detalle suficiente para analizar el riesgo y sostener la decisión que se pretende tomar.

La gestión de activos, accesos, adquisición y mantenimiento forma parte de las materias de NIS2. El CSF ayuda a ordenar la identificación; el SGIA conserva la relación con sistema, uso, datos, recursos e impactos. Las conexiones son funcionales y deben concretarse para cada alcance. [F1, F2]

2. Qué debe contener un inventario que sirva para decidir

Activo o dependencia	Información mínima útil	Pregunta de comprobación
Datos	Fuente, finalidad, versión, acceso, conservación y transformaciones relevantes	¿Podemos localizar los datos utilizados y justificar su tratamiento?
Modelo y software	Identificador, procedencia, versión y configuración pertinente	¿Podemos reconstruir qué se ejecutó?
Identidades	Titular o responsabilidad, permisos, finalidad y ciclo de vida	¿Se puede atribuir y revocar el acceso?
Infraestructura	Entorno, servicios, límites, operación y dependencias	¿Qué dejaría de funcionar si falla este componente?
Interfaces	Origen, destino, información intercambiada y permisos	¿Qué puede entrar, salir o activarse a través de ella?
Terceros	Servicio exacto, condiciones, contactos y responsabilidad compartida	¿Qué controlamos y qué necesitamos del proveedor?
Personas y operación	Función, formación, disponibilidad y suplencia	¿La supervisión y el escalado pueden realizarse en la práctica?
Registros y recuperación	Fuentes, acceso, integridad, disponibilidad y restauración	¿Podemos investigar y recuperar con lo conservado?

No todos los datos deben copiarse a H03. Puede bastar un localizador a un inventario existente. Se identifica qué registro tiene autoridad sobre cada dato y quién mantiene sus cambios. Una lista muy completa que nadie actualiza puede dar una seguridad falsa.

3. Dibujar relaciones, no solo enumerar objetos

Para cada relación registra origen, destino, datos o capacidad transferida, identidad utilizada y límite de confianza. Un límite de confianza separa contextos con distintos permisos o supuestos: por ejemplo, un archivo recibido de fuera y un entorno donde se ejecuta una prueba. No se da por fiable la información únicamente porque llegue por una herramienta conocida.

Supuesto adicional C3-DEP-01. Se define un ensayo aislado para estudiar dependencias: se recibe un conjunto de tickets sintéticos, se guarda una versión de entrada, se ejecuta un clasificador de evaluación, una persona revisa sus resultados y se conserva el informe. No se define una API generativa, un agente ni una conexión con producción. Es un diseño docente que no afirma la arquitectura real de SYS-003.

En ese supuesto, el mapa debe permitir recorrer: fuente sintética → recepción y control del archivo → conjunto versionado → ejecución identificada → revisión humana → informe y decisión. También señala cuentas, permisos y registros necesarios para cada paso. Si el informe no identifica el conjunto de entrada, la cifra final pierde capacidad para sostener una comparación.

4. Construir escenarios útiles

Una amenaza describe una posible fuente de daño o actuación. Una vulnerabilidad es una debilidad que puede facilitarlo. Un fallo puede surgir sin intención maliciosa. Un incidente requiere hechos sobre un compromiso o afectación que se evalúan conforme al marco pertinente. Estas categorías ayudan a investigar, pero no sustituyen la evidencia.

Escenario del supuesto	Qué habría que observar	Lo que no demuestra por sí solo
Se altera el archivo después de su recepción	Versiones, permisos, trazas y diferencias	Una diferencia de hash no identifica automáticamente al responsable ni su intención
Se confunde un conjunto de prueba con otro	Identificadores, protocolo, fecha y trazabilidad	La mejora del promedio no demuestra que las muestras sean comparables
Una cuenta puede modificar resultados e informe	Permisos efectivos y revisión de operaciones	Disponer del permiso no prueba que se haya utilizado indebidamente
La revisión humana no recibe un resultado	Cola, aviso, recepción y disponibilidad de la función	Un procedimiento escrito no demuestra que el aviso haya llegado
Se pierde un registro necesario para investigar	Disponibilidad, integridad, conservación y prueba de consulta	La ausencia de un evento en el registro no siempre demuestra que el evento no ocurrió

En otros sistemas podrían examinarse envenenamiento de datos, manipulación de entradas o exposición a través de una integración generativa. Para introducir esos escenarios se documenta antes el componente pertinente. No se atribuye una arquitectura al caso únicamente para poder explicar una amenaza de moda.

5. Comparar evidencias de integridad, procedencia y autorización

Una huella digital permite comparar contenido con una referencia. Su utilidad depende de que la referencia y el proceso de obtención sean fiables. Si quien altera un archivo puede sustituir también la huella de referencia, conservar ambas no demuestra autenticidad. La integridad del archivo, su procedencia y la autorización para utilizarlo son cuestiones relacionadas, pero distintas.

Del mismo modo, un identificador de modelo no reconstruye por sí solo todos los parámetros, datos o componentes que influyeron en una ejecución. Se selecciona la información necesaria para la finalidad del expediente. Una reconstrucción para depurar un error puede necesitar detalles diferentes de un registro mínimo de operación.

Conservar información tampoco justifica guardarlo todo indefinidamente. Se consideran acceso, minimización, obligaciones de conservación y necesidades de investigación. Los registros que contienen datos sensibles requieren protección y criterios de retención.

6. Priorizar qué comprobar

H03 vincula cada dependencia con un escenario, su evidencia y una decisión. Se comienza por las relaciones que pueden invalidar una conclusión importante o producir consecuencias relevantes. Si falta una pieza, se formula una comprobación concreta: «Confirmar qué conjunto se utilizó en esta ejecución y quién podía modificarlo». «Revisar la seguridad» es demasiado amplio para saber cuándo se ha terminado.

En Tech Server IIT Spain se mantienen los resultados v1 90/100 y 9/10 críticos; v2 94/100 y 7/10. El inventario debe ayudar a examinar comparabilidad y posibles causas sin darlas por establecidas. La v2 sigue probada, sin autorización de despliegue; v1 tampoco queda autorizada por comparación.

Actividad 1. Resolver un inventario incompleto

Enunciado: el inventario del ensayo lista el clasificador y el servidor, pero omite archivo de entrada, cuentas administrativas, revisión humana e informe.

Qué. Completar las dependencias necesarias para reconstruir la prueba y evaluar el riesgo de sus resultados.

Por qué. Esos elementos pueden alterar entradas, ejecución, interpretación o decisión aunque no sean el modelo.

Cómo. Recorrer entrada, procesamiento, salida y uso; identificar responsabilidades, permisos y fuentes de evidencia; vincular escenarios y pendientes.

Cuándo. Antes de cerrar la comparación o ampliar el alcance del ensayo.

Dónde. En H03 y en los inventarios existentes, conservando autoridad por dato y referencias a FD-001 y CAM-001.

Con qué. Protocolo, archivos versionados, configuración, permisos y personas que realizaron y revisaron la prueba.

Actividad 2. Un hash distinto no demuestra un ataque

Enunciado: dos copias tienen huellas distintas y se anuncia que un atacante manipuló el modelo, atribuyéndole además T10-014.

Qué. Registrar la diferencia y abrir comprobaciones de contenido, origen y cronología sin afirmar autoría ni relación causal.

Por qué. La diferencia puede tener varias explicaciones. No establece quién actuó, con qué intención o qué episodio resultó afectado.

Cómo. Preservar copias y contexto, comprobar referencias y transformaciones, identificar permisos y reconstruir la cadena. T10-014 conserva sus incógnitas hasta contar con evidencia pertinente.

Cuándo. Al detectar la discrepancia, evitando perder fuentes durante la investigación.

Dónde. En H03 y en los expedientes de cambio o incidente que correspondan, con hechos e hipótesis diferenciados.

Con qué. Copias preservadas, huellas fiables, registros, procedimiento de obtención y revisión competente.

Comprueba lo aprendido

1. ¿Una dependencia humana puede formar parte del mapa? Sí.
2. ¿Un hash prueba autorización de uso? No.
3. ¿Un permiso excesivo demuestra una acción indebida? No, aunque exige evaluar y tratar el riesgo.
4. ¿Debe atribuirse una API generativa a SYS-003 para hablar de seguridad? No.

Evidencia de salida

Completa H03 con al menos cinco dependencias, sus relaciones y dos escenarios. Identifica una afirmación que todavía no pueda sostenerse y la comprobación que ayudaría a resolverla.

Fuentes

F1. NIS2, artículo 21 y definiciones pertinentes.

F2. NIST CSF 2.0.

F3. ENISA: guía técnica NIS2, 2025, como apoyo dentro de su alcance. El mapa y los supuestos son elaboraciones docentes originales.

Clase de audio 045

045. NIS2 y NIST CSF 2.0: gobierno de IA y responsabilidad directiva

Aclaraciones para aplicar esta clase

Utiliza estas cuatro claves al resolver los ejercicios de gobierno, prioridades y evidencias:

1. **Responsabilidad y formación.** Las tareas operativas pueden distribuirse y delegarse dentro de la autoridad asignada. Esa organización no extingue las responsabilidades de aprobación y supervisión atribuidas al órgano de dirección por el régimen aplicable. La referencia del artículo 4 del AI Act es su redacción modificada por el Reglamento (UE) 2026/1744: una norma aprobada, no una modificación solo proyectada. Las cinco horas del ejemplo son una propuesta formativa interna, no un mínimo legal.

2. **Evidencia y trazabilidad.** Un documento no aportado o no revisado se registra como no acreditado; no se afirma por ello que no exista. Si falta información necesaria de una prueba, se identifica qué conclusiones quedan limitadas y cómo obtener soporte suficiente. No se valida una conclusión que dependa de un dato ausente ni se anula automáticamente toda utilidad del ensayo. C3-DEP-01 es un ensayo adicional y no documenta la arquitectura completa de SYS-003.

3. **Cierre de acciones.** El cierre depende del resultado y del criterio establecido. Un correo puede aportar evidencia de una comunicación concreta; su envío no demuestra por sí solo que se haya resuelto otra carencia técnica u organizativa. Se comprueban alcance, contenido y resultado pertinentes.

4. **Rendimiento y autorización.** La caída en críticos debe evaluarse con criterios previos, finalidad y evidencia; no representa un umbral universal de NIS2 o ISO. v2 continúa probada, sin autorización de despliegue, y v1 no se autoriza por comparación. La trazabilidad acompaña a la calidad, la prevención y la respuesta: no las sustituye.

Referencias: NIS2, artículo 20 y Reglamento (UE) 2026/1744, modificación del artículo 4 del AI Act.

CURSO SGIA · MONOGRÁFICO 3

Identificar la cadena del servicio

NIS2 + NIST CSF 2.0 · Lección 3

01 Datos y componentes con versión

Identifica procedencia y configuración para reconstruir una ejecución y sus resultados.

02 Identidades, personas y terceros

Incluye quienes supervisan, operan y prestan servicios, con sus responsabilidades.

03 Relaciones y límites de confianza

Recorre entradas, transformación, salida y uso. Comprueba permisos y autoridad de los datos.

04 Escenarios como hipótesis comprobables

Una diferencia o un permiso no demuestran ataque: formula la comprobación que falta.

TU EVIDENCIA DE SALIDA

H03: mapa de dependencias y evidencias

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 3. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 4. Proteger datos, identidades y configuraciones

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Seleccionar medidas según el riesgo, comprobar accesos y cambios y preparar pruebas que permitan concluir algo concreto. Trabajo orientativo: 100 minutos, incluida la ficha H04.

1. Una medida necesita una función y una prueba

«Tenemos cifrado» no explica qué información se protege, dónde, frente a qué exposición ni quién puede descifrarla. «Usamos doble factor» no describe todas las identidades de una integración. Para valorar una medida necesitamos conocer su alcance y qué resultado se ha comprobado.

NIS2 contempla medidas técnicas, operativas y de organización adecuadas y proporcionadas al riesgo, incluyendo accesos, activos, adquisición y mantenimiento, criptografía, formación y continuidad. Las decisiones no se limitan a comprar productos. En el SGIA deben conectarse con datos, recursos, ciclo de vida y uso de la IA. [F1]

H04 recoge el recorrido **riesgo → medida → criterio → prueba → resultado → decisión**. Si falta el criterio, puede ocurrir que cualquier resultado parezca aceptable. Si falta la prueba, una descripción de diseño se puede confundir con un control que funciona.

2. Identidades humanas y de servicio

Una cuenta humana identifica a una persona; una identidad de servicio permite que un componente actúe. Ambas necesitan responsabilidad y límites, pero no se gestionan necesariamente con el mismo mecanismo. Pedir a una API que introduzca un código de una aplicación móvil no describe una solución operativa para todas las identidades técnicas.

Se identifica quién solicita y autoriza el acceso, para qué finalidad, sobre qué entorno y durante cuánto tiempo. Se aplica el permiso necesario y se comprueba qué puede hacer realmente la identidad. También se prepara su retirada, sustitución y revisión. Una cuenta deshabilitada en una pantalla puede conservar sesiones o credenciales que haya que examinar.

Para accesos privilegiados se valoran controles reforzados, autenticación adecuada, atribución y supervisión. El artículo 21.2.j contempla autenticación multifactorial o continua y comunicaciones seguras en los términos pertinentes; el diseño concreto depende del riesgo y la aplicabilidad. No se da por protegido todo el servicio porque una sola cuenta tenga MFA.

En el supuesto C3-ALC-01 hay dos cuentas administrativas y una carece de responsable registrado. No se decide eliminarla automáticamente: antes se comprueban uso y dependencias, se elige la medida y se prueba que no se rompe un acceso necesario ni se mantiene otro sin justificación.

3. Credenciales y secretos

Una clave puede aparecer en archivos, historiales, registros, capturas o paquetes compartidos. El procedimiento debe evitar que resolver una incidencia propague el secreto. Los ejemplos del curso utilizan valores ficticios; nunca se necesitan credenciales reales para completar una actividad.

Pregunta	Evidencia que permite responder
¿Quién responde de esta identidad técnica?	Registro de responsabilidad y finalidad

Pregunta	Evidencia que permite responder
¿Qué permisos tiene realmente?	Configuración y ensayo controlado pertinente
¿Dónde se almacena su secreto y quién accede?	Diseño, permisos y revisión del almacenamiento
¿Puede revocarse sin perder el servicio legítimo?	Plan de sustitución, ensayo y resultado
¿Qué ocurre si se expone?	Procedimiento de contención, revisión de usos y recuperación

La rotación puede formar parte del tratamiento, pero una frecuencia elegida sin contexto no garantiza seguridad. Importa también si la clave antigua deja de servir, si se eliminan copias indebidas y si los accesos posteriores son atribuibles. Un registro de «clave cambiada» no acredita todas esas condiciones.

4. Protección de datos durante su recorrido

Se revisan captura, transmisión, almacenamiento, transformación, uso y eliminación. En cada paso se pregunta qué información se necesita, quién puede verla y qué exposición o alteración se debe evitar. La minimización no consiste en borrar campos al azar: debe preservar la finalidad legítima y la capacidad de evaluar el sistema.

Los datos de evaluación necesitan protección y trazabilidad. Si se altera una etiqueta de referencia, la métrica puede dejar de medir lo que creemos. Separar conjuntos y responsabilidades, controlar cambios y conservar información de procedencia puede reducir riesgos de confusión o manipulación. La selección se justifica por el proceso real.

El cifrado necesita gestión de claves y acceso autorizado. Una copia cifrada inaccesible para quien debe recuperar el servicio puede ser un problema de continuidad. Una salida descifrada y enviada al destinatario equivocado puede seguir siendo una exposición aunque el almacenamiento previo estuviera cifrado. La medida se evalúa en el recorrido completo pertinente.

5. Configuración y cambios seguros

La línea de referencia identifica qué configuración se considera válida para un entorno y uso. Incluye los elementos necesarios para reconstruir y comprobar un cambio: versiones, dependencias, permisos, reglas de datos, registros y supervisión. No se presupone que SYS-003 tenga parámetros de un modelo generativo.

Un cambio debe permitir responder: qué modifica, por qué, qué riesgos e impactos altera, qué pruebas se necesitan, quién decide y cómo se revierte o contiene si falla. La reversión requiere comprobar que la versión o configuración anterior sigue siendo apropiada; no basta con que antes funcionara.

En un sistema hipotético adicional con agentes, el análisis incluiría permisos de herramientas, límites de acciones y validación de operaciones relevantes. En un clasificador sin esas capacidades, esos controles no se imponen como si fueran parte de su arquitectura. La plantilla conserva campo de aplicabilidad y justificación.

6. Supuesto adicional C3-PRO-01: probar una revocación

Se crea una integración de ensayo con datos sintéticos y una clave ficticia. El objetivo interno es comprobar que la clave revocada deja de permitir llamadas y que una alternativa autorizada conserva la operación necesaria. No se ha definido una integración real de SYS-003.

El ensayo identifica entorno, claves por referencia no secreta, permisos y operaciones. Se verifica una operación permitida antes del cambio, se revoca la clave de ensayo y se comprueba su rechazo. Se ensaya

después la alternativa autorizada. Se conservan resultado y limitaciones sin copiar secretos a H04.

Si la llamada con la clave revocada sigue funcionando, el control no se cierra por haber pulsado «revocar». Se examinan caché, sesión, demora documentada, credencial utilizada y otros factores. Si la alternativa tampoco funciona, hay además una carencia de continuidad. Cada conclusión requiere su evidencia.

Actividad 1. Diseñar una prueba con resultado verificable

Enunciado: H04 solo contiene «activar controles de acceso» y una captura del panel.

Qué. Añadir alcance, criterio de aceptación y ensayo de permisos efectivos.

Por qué. La captura puede describir configuración, pero no prueba por sí sola el comportamiento que se necesita.

Cómo. Identificar identidad y operación, definir qué debe permitir y rechazar, preparar ensayo controlado y registrar resultados y límites.

Cuándo. Antes de declarar resuelta la brecha o autorizar el cambio.

Dónde. En H04, con enlaces a la configuración y CAM-001.

Con qué. Entorno autorizado, datos de ensayo, permisos comprobados y criterio previo.

Actividad 2. Una reversión también necesita decisión

Enunciado: ante un problema se propone desplegar v1 porque detectó 9/10 críticos y retirar v2, sin revisar autorizaciones.

Qué. Comprobar el estado y la adecuación de las alternativas sin autorizar ninguna versión por comparación.

Por qué. La mejor cifra relativa no acredita seguridad, calidad suficiente ni autorización de uso. v2 permanece probada, sin autorización de despliegue.

Cómo. Identificar versión realmente utilizada, requisitos y decisiones; valorar medidas de continuidad adecuadas y someter la opción a la autoridad correspondiente. No asumir que v2 estuviera en producción.

Cuándo. Al preparar continuidad y ante una decisión efectiva de cambio.

Dónde. En CAM-001 y en el expediente operativo y de incidentes que corresponda.

Con qué. Fuentes autorizadas del estado, pruebas pertinentes y responsables con autoridad.

Comprueba lo aprendido

1. ¿Configurar una medida demuestra su eficacia? No: se comprueba el resultado pertinente.
2. ¿Deben copiarse claves reales a la ficha? No.
3. ¿El cifrado resuelve por sí solo destinatarios y finalidad? No.
4. ¿Una reversión evita revisar riesgos y autorización? No.

Evidencia de salida

Completa H04 con dos medidas y sus pruebas: una sobre accesos y otra sobre datos o configuración. Debe distinguirse qué se propuso, qué se ejecutó, qué se observó y qué decisión existe realmente.

Fuentes

NIS2, artículo 21, NIST CSF 2.0 y guía técnica ENISA. Las medidas y pruebas descritas son propuestas docentes que se adaptan al riesgo y al alcance.

CURSO SGIA · MONOGRÁFICO 3

Proteger con medidas comprobadas

NIS2 + NIST CSF 2.0 · Lección 4

01 **Permisos y finalidad de cada identidad**

Diferencia identidades humanas y técnicas. Comprueba permisos efectivos y revocación.

02 **Datos protegidos en todo el recorrido**

Minimiza y controla acceso, transmisión, conservación y eliminación según el uso.

03 **Cambios con referencia y autorización**

Identifica qué cambia, por qué y quién puede decidir. Prepara una alternativa comprobable.

04 **Prueba previa, resultado y límites**

Una captura no demuestra eficacia. Separa diseño, ejecución, observación y decisión.

TU EVIDENCIA DE SALIDA

H04: riesgo, medida, ensayo y decisión

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 4. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 5. Gestionar proveedores y cadena de suministro

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Evaluar una dependencia de IA, repartir actuaciones con terceros y decidir qué evidencia falta antes de proponer su autorización. Trabajo orientativo: 100 minutos con el cuestionario H05.

1. Comprar un servicio no elimina la responsabilidad propia

Un proveedor controla una parte del servicio; nuestra organización decide cómo lo integra, qué datos le envía, qué permisos concede y cómo utiliza sus resultados. Para gobernar la dependencia necesitamos conocer ambas partes. «Lo gestiona el proveedor» puede describir una tarea, pero no responde si la organización conserva capacidad suficiente para cumplir sus obligaciones.

NIS2 contempla seguridad en la relación con proveedores directos y consideración de sus vulnerabilidades y prácticas pertinentes. GV.SC del CSF organiza el trabajo de cadena de suministro. En el SGIA la conexión principal está en las relaciones con terceros y clientes, área A.10; el área A.7 complementa el análisis de datos. Estas conexiones no convierten una ficha en una declaración automática de cumplimiento. [F1-F3]

2. Evaluar lo que se adquiere realmente

Modalidad	Dependencias que conviene examinar
API remota	Identidad y permisos, datos enviados y conservados, versiones, disponibilidad, avisos, límites y colaboración ante incidentes
Fine-tuning	Lo anterior cuando proceda, más procedencia y permisos de datos de ajuste, aislamiento, artefactos, acceso y exposición
Modelo de terceros incorporado	Origen, versión, integridad, licencia, dependencias, soporte, pruebas y operación propia
Servicio gestionado que utiliza IA	Responsabilidades del servicio completo, información necesaria, coordinación, continuidad y límites de supervisión

La presencia de IA no justifica aplicar sin más las mismas preguntas a todas las modalidades. Si una cuestión no corresponde, se documenta por qué. Si no conocemos la respuesta, se deja como carencia de evidencia, no como no aplicable.

La denominación comercial de «proveedor» tampoco fija automáticamente el rol jurídico del AI Act. Al analizar ese marco se examinan finalidad, actuaciones y condiciones que correspondan. Una relación contractual no permite omitir el análisis de roles trabajado en el primer monográfico.

3. Combinar documentos y pruebas propias

Una certificación puede aportar información sobre un alcance y periodo determinados. El contrato define compromisos; la documentación técnica describe el servicio; las pruebas propias muestran una parte del comportamiento de la integración. Ninguna de esas fuentes responde por sí sola a todo.

Antes de utilizar un certificado se comprueban emisor, alcance, vigencia y exclusiones. Un informe sobre un centro de datos no demuestra automáticamente cómo se utilizan los contenidos enviados a una API. Las

condiciones de una modalidad empresarial no se trasladan sin comprobarlas a una cuenta distinta.

Las pruebas también tienen límites. Un ensayo con diez solicitudes sintéticas puede verificar un rechazo de permisos, pero no demostrar ausencia de exposición en todos los usos. Una prueba de funcionamiento no demuestra que el contrato cubra la finalidad de los datos. Se explicita qué conclusión sostiene cada evidencia.

4. Supuesto adicional C3-SUP-01

Se propone una API de asistencia de **Proveedor Delta**, nombre ficticio, para un uso adicional separado de SYS-003. El alcance no incluye fine-tuning ni descarga del modelo. Las condiciones simuladas no aclaran suficientemente reutilización y retención de documentación interna; existe soporte genérico, pero falta coordinación urgente probada.

El cuestionario H05 contiene veinte preguntas. En el ejemplo cumplimentado, Q07 mantiene una carencia decisiva sobre datos y Q17 una sobre incidentes. Se propone dejar pendiente la autorización de ese uso con documentación interna real. No se presenta al proveedor como inseguro en todos sus servicios: la conclusión se limita al alcance y evidencia del ejercicio.

Una alternativa con datos sintéticos podría reducir una parte de la exposición, pero requiere alcance, permisos y autorización propios. No prueba por sí sola la adecuación de un uso posterior con datos reales. Tampoco se inventa una autorización para continuar el ensayo.

5. Qué debe acordarse para gestionar incidentes

La organización necesita saber qué información obtendrá, quién avisará, por qué canal, con qué disponibilidad y cómo colaborará cada parte. El acuerdo se contrasta con nuestras obligaciones: si un aviso llega tarde o carece del contenido necesario, puede dificultar la evaluación y comunicación propias.

No se impone al proveedor el plazo de 72 horas como si resolviera todos los casos. El reloj de nuestra entidad puede empezar cuando tenga constancia del incidente significativo; las obligaciones del tercero y los compromisos contractuales se analizan por separado. La coordinación debe permitir actuar dentro de los requisitos que correspondan a cada parte.

Una dirección genérica de soporte no acredita una vía de emergencia operativa. Puede ensayarse el contacto, la suplencia y la disponibilidad de la información, utilizando un ejercicio autorizado que no provoque una alerta real ni comparta datos sensibles innecesarios.

6. Cambios durante la relación

La evaluación inicial tiene fecha y alcance. Cambiar modelo, ubicación de datos, subproveedor, permisos, finalidad o condiciones puede invalidar parte de su fundamento. Se identifica qué cambios deben avisarse, quién los examina y qué pruebas se repiten.

No toda modificación requiere el mismo esfuerzo. Una corrección limitada y bien documentada puede necesitar comprobaciones distintas de una ampliación de permisos. El método debe permitir justificar esa diferencia. Una etiqueta «actualizado» sin identificación de versión dificulta reconstruir una decisión posterior.

El seguimiento conserva evidencias de cambios, desempeño, incidentes, carencias y medidas. Se relaciona con PROV-001, CAM-001 y MON-001. Copiar el nombre del proveedor a varios archivos no crea trazabilidad si cada copia muestra un estado diferente sin autoridad definida.

7. Preparar la salida antes de necesitarla

El fin del servicio puede dejar datos, accesos, modelos ajustados, registros o una dependencia operativa. Se identifican actividades de devolución, exportación pertinente, retirada de permisos, conservación justificada y borrado verificable cuando corresponda. La salida se vincula a continuidad, requisitos y responsabilidades.

No siempre es posible sustituir inmediatamente un proveedor. Esa dificultad debe formar parte del riesgo y de la decisión, con alternativas y límites. Un plan que promete migrar en una hora sin haber probado

dependencias no ofrece una base suficiente para gobernar la continuidad.

H05 evita compensar una carencia decisiva con muchos puntos favorables. La conclusión es una propuesta razonada: autorización para alcance definido, pendiente de carencias o rechazo propuesto. La decisión corresponde a la autoridad identificada. La evaluación de un proveedor no autoriza el despliegue de SYS-003 v2.

Actividad 1. Interpretar «cero retención»

Enunciado: una página comercial menciona cero retención, pero el contrato del servicio evaluado y su configuración no permiten comprobar si esa condición se aplica a nuestra cuenta.

Qué. Registrar información parcial y mantener pendiente la conclusión sobre conservación para ese alcance.

Por qué. Un mensaje general puede corresponder a otra modalidad o tener condiciones que no se han verificado.

Cómo. Identificar producto y cuenta, obtener términos aplicables, revisar configuración y evidencias pertinentes y documentar diferencias y límites.

Cuándo. Antes de enviar los datos del uso propuesto y cuando cambien las condiciones.

Dónde. En H05 y PROV-001, enlazados al expediente de datos y riesgos.

Con qué. Documentación contractual y técnica del servicio exacto, configuración y revisión competente.

Actividad 2. Reutilizar una aprobación antigua

Enunciado: se quiere ampliar la API para ejecutar acciones sobre otra herramienta porque el proveedor ya fue evaluado como asistente de lectura.

Qué. Abrir la revisión del cambio de alcance antes de habilitar nuevas capacidades.

Por qué. La evaluación de lectura no demuestra adecuación de permisos para actuar ni de la supervisión de esas acciones.

Cómo. Describir operaciones y límites, analizar riesgos e impactos, revisar datos y responsabilidades, probar permisos y controles y solicitar la decisión pertinente.

Cuándo. Antes de conceder los nuevos permisos.

Dónde. En CAM-001 y H05, manteniendo la evaluación original y su alcance.

Con qué. Mapa de dependencias, condiciones del proveedor, pruebas propias y fuente autorizada del estado.

Comprueba lo aprendido

1. ¿No evidenciado significa que el proveedor carezca del control? No.
2. ¿Una certificación cubre todas las modalidades del servicio? Hay que comprobar su alcance.
3. ¿Un contrato aceptado autoriza el despliegue de IA? No por sí solo.
4. ¿La salida debe pensarse únicamente al terminar? No: se prepara como parte del gobierno de la dependencia.

Evidencia de salida

Completa las veinte preguntas H05 para un servicio real sin incluir secretos o utiliza el supuesto simulado. Justifica las respuestas no aplicables, identifica carencias decisivas y redacta una propuesta de decisión con límites y evidencia de cierre.

Fuentes

F1. NIS2, artículo 21.2.d y 21.3.

F2. NIST SP 1305, apoyo para organizar la capacidad de gestión de cadena de suministro y definir requisitos.

F3. ISO/IEC 42001 y presentación institucional UNE sobre sus áreas de control.

Clase de audio 046

046. NIS2 y NIST CSF 2.0: protección y proveedores de IA

Claves para aplicar esta clase

Utiliza estas cinco claves al resolver las actividades de protección y proveedores:

1. **Datos y fine-tuning.** Que el servicio contratado no incluya fine-tuning no garantiza que el proveedor no conserve o reutilice documentos. Q12 y Q13 no aplican al alcance actual, mientras Q07 sigue sin evidencia suficiente. Se revisan condiciones, configuración, accesos y conservación. Fine-tuning es entrenamiento adicional de un modelo; pedir otro tono de respuesta no implica necesariamente ese entrenamiento.

2. **Riesgos y cambios.** Una API de lectura puede exponer información o producir respuestas que influyan en decisiones importantes; el daño no queda necesariamente confinado al resumen. Al añadir acciones se evalúan sus capacidades y se eligen límites, supervisión y parada según riesgos y requisitos. No existe una regla universal de confirmación humana antes de toda acción. La evidencia anterior se conserva si sigue vigente y es pertinente.

3. **Soporte y salida.** Q17 acredita soporte genérico, pero deja incompleta la coordinación urgente; no demuestra ausencia de atención ni espera hasta el lunes. Q20 requiere completar exportación, conservación justificada y eliminación cuando corresponda, con alcance, plazos y soporte suficiente. No se promete comprobar directamente el borrado irreversible de toda copia remota ni alcanzar certeza absoluta.

4. **Marco y responsabilidades.** NIS2 se aplica dentro de su ámbito; usar IA no basta para determinarlo. NIST CSF organiza resultados y no crea por sí solo obligaciones legales universales. NIST no certifica implementaciones del CSF. El contrato puede incorporar controles y obligaciones; distribuir tareas no elimina las obligaciones propias de cada parte. A.10 y A.7 conectan funcionalmente terceros y datos en el SGIA.

5. **Pruebas y decisiones.** El ensayo de revocación continúa sin resultado de ejecución aportado. Los ejemplos temporales y de ataque de la conversación no son hechos del caso. Q09 es una prueba favorable simulada de otro expediente; no ejecuta el primer plan. La autoridad competente debe autorizar el ensayo en su alcance. El uso propuesto de Delta con documentación interna real sigue pendiente hasta resolver las carencias pertinentes de Q07, Q17 y Q20 y obtener la decisión correspondiente. El objetivo es evidencia suficiente y proporcional para decidir.

Referencias: NIS2, artículo 21; NIST CSF, preguntas frecuentes; NIST, fine-tuning; OWASP, información sensible en aplicaciones LLM.

CURSO SGIA · MONOGRÁFICO 3

Gobernar la dependencia del proveedor

NIS2 + NIST CSF 2.0 · Lección 5

01 Servicio exacto, datos y permisos

Evalúa la API o componente contratado, sus modalidades y los datos que recibirá.

02 Contratos y pruebas con alcance

Comprueba vigencia y límites. Un certificado no valida toda la integración.

03 Avisos, cambios e incidentes coordinados

Prepara información y contactos que permitan actuar dentro de nuestras obligaciones.

04 Continuidad y salida previstas

Define recuperación, retirada de permisos y tratamiento de datos al terminar la relación.

TU EVIDENCIA DE SALIDA

H05: veinte preguntas y carencias decisivas

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 5. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 6. Detectar señales y comprobar la vigilancia

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Definir señales y responsabilidades, comprobar que los registros llegan y que los avisos pueden ser atendidos, e interpretar métricas sin ocultar puntos ciegos. Trabajo orientativo: 100 minutos.

1. Tener registros no equivale a detectar

Un archivo puede contener el evento correcto y no existir ninguna regla que lo reconozca. Una regla puede generar una alerta que nadie recibe. Una alerta recibida puede quedar sin triaje porque no hay suplente. La detección útil incluye esas relaciones y no termina al comprar una plataforma.

La función Detectar del CSF ayuda a ordenar observación y análisis; el trabajo se conecta con respuesta, gobierno y protección. En el SGIA, MON-001 conserva seguimiento y resultados e INC-001 organiza los incidentes cuando corresponda. El seguimiento de rendimiento del modelo y la vigilancia de seguridad se relacionan, pero tienen objetivos y evidencias distintos. [F1, F2]

2. Empezar por una pregunta de riesgo

Una señal se define porque ayuda a observar un escenario relevante. «Guardar todos los datos» no explica qué se busca y puede aumentar exposición, costes y dificultades de investigación. La ficha H06 identifica escenario, fuente, condición de alerta, responsable, acción prevista y prueba.

Escenario	Señal posible, a adaptar	Comprobación necesaria
Cambios de permisos no previstos	Operación de concesión o modificación	Permiso previo y posterior, identidad, autorización y contexto
Pérdida de vigilancia	Ausencia de recepción esperada o fallo del colector	Fuente y periodo cubiertos; distinguir falta de eventos de falta de registro
Uso de una clave revocada	Intento posterior al hito de revocación	Credencial por referencia, momento y resultado; no copiar su valor secreto
Alteración de un artefacto	Diferencia respecto de referencia controlada	Contenido, origen y proceso de cambio; no asumir intención maliciosa
Salida o uso fuera del alcance permitido	Evento pertinente del flujo	Finalidad, destinatario, contenido y autorización, si el sistema permite observarlos

Una señal puede necesitar información de varias fuentes. También puede no estar disponible técnicamente. Se registra la limitación y se evalúan alternativas; no se declara vigilancia de un riesgo solo porque aparezca en un catálogo.

3. Conservar contexto para investigar

Un registro útil puede necesitar identificador de evento, servicio y entorno, versión o configuración relevante, identidad atribuible, fecha y zona horaria, operación y resultado. Se decide qué datos son necesarios y cómo protegerlos. La capacidad de reconstrucción depende además de sincronización, conservación, integridad y acceso.

Una marca temporal no es automáticamente exacta. Si dos fuentes usan zonas o relojes distintos, la cronología puede ordenar mal los hechos. Se preserva la hora original, se documenta la conversión y se investiga la fiabilidad cuando importe para la conclusión. No se corrige una marca sobrescribiendo el dato original sin historial.

Los registros pueden contener datos personales, contenido interno o secretos. Se definen permisos, retención y acceso para investigación. Si un incidente requiere compartir información, se transmite lo pertinente por el canal adecuado, no una copia indiscriminada de todo el sistema.

4. Comprobar toda la cadena

Una prueba autorizada identifica el evento que se generará, el entorno, qué resultado se espera en cada etapa y cómo se evitará un efecto real no deseado. Puede utilizar datos sintéticos y canales de ejercicio. Probar no exige provocar un ataque real ni habilitar producción sin autorización.

La cadena que examinaremos es: **evento de prueba → registro recibido → alerta generada → aviso recibido por la función responsable → triaje y actuación**. Se comprueba también qué ocurre cuando la cadena se rompe. Una prueba de caída de recepción puede ser tan importante como otra que demuestre una regla de alerta.

Supuesto adicional C3-DET-01

Se generan diez eventos sintéticos identificados y pertinentes para una regla del entorno de ensayo. Las etapas son anidadas: nueve llegan al colector; de esos nueve, ocho generan alerta; de esas ocho, siete llegan a la función de guardia. No se describen incidentes reales de Tech Server IIT Spain.

Etapa	Resultado	Proporción respecto de los diez eventos previstos
Registro recibido	9 de 10	90 %
Alerta generada	8 de 10	80 %
Aviso recibido por la función prevista	7 de 10	70 %

La cifra de 90 % no describe el resultado completo hasta la guardia. Si se informa de eficacia de la regla solo sobre registros recibidos, el cociente sería 8/9 y habría que identificar ese denominador. Ninguna de esas cifras mide por sí sola la cobertura de todos los activos o amenazas de la empresa.

El ensayo tampoco permite calcular una tasa de falsas alarmas: se han descrito eventos de prueba que debían detectarse, no una muestra pertinente de eventos que no debían generar alerta. No se inventa un resultado de cero falsos positivos.

5. Tiempo de detección y respuesta

Definir «tiempo de detección» requiere fijar evento inicial y hito final. Puede medirse desde la generación controlada hasta la alerta, o desde la recepción del registro hasta el análisis, según la finalidad. Cada indicador debe declarar su definición, población, exclusiones y fuente.

Si se calcula la latencia únicamente de siete avisos recibidos, el indicador debe decirlo. Los tres que no completaron la cadena no tienen latencia cero. Se registran como fallos o casos sin hito final y se informa de

su efecto. Un promedio favorable de los que llegaron puede ocultar pérdidas de cobertura.

Las reglas internas de aviso o escalado se justifican según riesgo y capacidad. No se presentan como nuevos plazos legales de NIS2. Los relojes jurídicos de comunicación se analizan en la lección 7 y no se sustituyen por los indicadores del panel.

6. De la señal al triaje

El triaje identifica qué se conoce, qué podría estar afectado, qué protección es necesaria y quién debe investigar. No tiene que resolver la causa raíz para comenzar a actuar. Diferencia una alarma de un incidente acreditado y una posible significatividad de una clasificación jurídica ya sustentada.

En H06 se define qué señales se escalan, con qué información mínima y a quién. Una ausencia de alerta no demuestra ausencia de incidente si la recepción de registros o la regla no funcionan. Del mismo modo, una alerta no demuestra por sí sola ataque o daño.

Se conserva evidencia de los ensayos y de las carencias. Una regla modificada necesita la comprobación pertinente; cerrar un ticket de configuración no demuestra que la cadena vuelva a funcionar. La nueva prueba conserva alcance e identificadores para que la comparación sea explicable.

Actividad 1. Corregir el panel de cobertura

Enunciado: se publica «detección del 90 %» usando solo los nueve registros recibidos de C3-DET-01 y se omite que siete avisos llegaron a la guardia.

Qué. Separar resultados de recepción, alerta y entrega y limitar la conclusión al ensayo.

Por qué. La cifra elegida no representa la cadena completa ni la cobertura de la organización.

Cómo. Mostrar 9/10, 8/10 y 7/10 con etapas e identificadores; investigar las pérdidas y repetir la prueba pertinente tras corregirlas.

Cuándo. Antes de comunicar eficacia o cerrar la carencia.

Dónde. En H06 y MON-001, con referencias al ensayo y sus resultados.

Con qué. Eventos identificados, registros, alertas y justificantes de recepción de la función de guardia.

Actividad 2. Interpretar un silencio

Enunciado: durante una franja no hay alertas y se concluye que no hubo actividad indebida, aunque no se comprobó que llegasen registros.

Qué. Declarar el límite de observación y comprobar la cadena antes de sostener ausencia de actividad.

Por qué. El silencio puede corresponder a falta de eventos o a una pérdida de vigilancia.

Cómo. Revisar disponibilidad de fuentes y recepción, ejecutar una comprobación autorizada y analizar el periodo afectado con las evidencias disponibles.

Cuándo. Al detectar la ausencia esperada o revisar el periodo.

Dónde. En MON-001; abrir o vincular INC-001 si los hechos y el procedimiento lo justifican.

Con qué. Fuentes originales, estado de colectores, reglas y ensayo controlado.

Comprueba lo aprendido

1. ¿Una alerta generada garantiza que alguien la recibió? No.
2. ¿Se pueden medir falsas alarmas con el supuesto descrito? No con esa información.
3. ¿Un aviso no recibido tiene latencia cero? No.
4. ¿El tiempo interno de escalado sustituye el reloj legal? No.

Evidencia de salida

Completa H06 para una señal y para la pérdida de su propia fuente de registro. Define responsable, suplente, prueba, resultados por etapa y acción ante fallo. Evita afirmar cobertura fuera del alcance comprobado.

Fuentes

F1. NIST CSF 2.0.

F2. NIS2, artículos 21 y 23.

F3. ENISA: guía técnica NIS2. Los indicadores y datos del ensayo son elaboraciones docentes, no umbrales legales ni resultados de la empresa.

CURSO SGIA · MONOGRÁFICO 3

Detectar y comprobar la vigilancia

NIS2 + NIST CSF 2.0 · Lección 6

01 Evento identificado y registro recibido

La fuente y su disponibilidad forman parte de la vigilancia. Un silencio necesita contexto.

02 Alerta generada para el escenario

Una regla debe reconocer el escenario pertinente y conservar el soporte de la alerta.

03 Aviso recibido y función disponible

Generar una alerta no acredita recepción ni atención. Comprueba también las suplencias.

04 Denominadores y puntos ciegos visibles

En el ensayo: 90 % registro, 80 % alerta y 70 % entrega respecto de diez eventos.

TU EVIDENCIA DE SALIDA

H06: diez eventos, nueve registros, ocho alertas, siete avisos

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 6. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 7. Responder, investigar y decidir las comunicaciones

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Coordinar respuesta y preservación de evidencia, evaluar significatividad y reconstruir los relojes de comunicación. Trabajo orientativo: 120 minutos con H07 y el supuesto resuelto.

1. Responder mientras se investiga

Ante una señal relevante puede ser necesario proteger un servicio o a sus usuarios antes de conocer la causa definitiva. El procedimiento debe permitir actuar con información limitada, conservar evidencia y revisar las decisiones a medida que se aclaran los hechos. Esperar una explicación perfecta puede agravar el daño o incumplir una comunicación exigible.

Contener, investigar y comunicar son trabajos relacionados. Se identifica quién coordina, quién puede aplicar medidas, quién conserva evidencia y quién está autorizado a remitir comunicaciones. Las suplencias y accesos al canal se preparan antes de necesitarlos. La RACI no sustituye la responsabilidad legal de la entidad ni del órgano correspondiente. [F1]

2. Diferenciar hechos, hipótesis y decisiones

En INC-001 cada afirmación relevante debe poder relacionarse con su fuente. «El servicio no responde» puede ser un hecho observado en un alcance; «hubo un ataque» es una hipótesis que necesita evidencia adicional. «Aislamos una dependencia» describe una decisión o actuación que debe tener hora, responsable y fundamento.

La preservación busca mantener información necesaria sin propagar secretos ni paralizar indiscriminadamente la protección. Se registran origen, obtención, acceso, transformaciones y limitaciones pertinentes de las evidencias. Una huella puede ayudar a comprobar integridad; no acredita por sí sola la veracidad de todo su contenido ni la identidad de quien lo generó.

No se reconstruye retrospectivamente una historia para que encaje con una conclusión inicial. Si un dato cambia, se conserva la revisión y su fundamento. La fuente autorizada se define por dato y alcance, no por el archivo cuya fecha sea más reciente.

3. Cuándo se analiza la significatividad

El artículo 23.3 de NIS2 contempla perturbaciones operativas graves o pérdidas económicas causadas o posibles para la entidad, y perjuicios materiales o inmateriales considerables causados o posibles a otras personas. Se revisan además las concreciones aplicables a la entidad y servicio. No existe un porcentaje universal de errores de IA que resuelva ese análisis. [F1]

Para las entidades comprendidas en el Reglamento 2024/2690 se examinan los artículos 3 y 4 y el artículo sectorial que corresponda. El criterio financiero común utiliza pérdidas directas superiores al menor importe entre 500.000 euros y el 5 % del volumen de negocios total anual del ejercicio anterior. Existen otros criterios suficientes; no superar esa cuantía no permite descartar todos. [F2]

En servicios gestionados y de seguridad gestionados, el artículo 10 incluye indisponibilidad completa durante más de treinta minutos. También contempla disponibilidad limitada con condiciones de usuarios y duración y determinados compromisos de integridad, confidencialidad o autenticidad. H07 desarrolla las condiciones exactas y sus diferencias. No se trasladan a todo servicio de IA sin verificar ámbito.

Un fallo accidental puede ser relevante para seguridad y continuidad. Una fuga puede abrir otras rutas jurídicas. Ni «no parece ataque» ni «solo es un problema del algoritmo» bastan para cerrar la evaluación.

4. Los relojes que no deben confundirse

Se diferencia primera detección de momento de constancia del incidente significativo. Este último no se desplaza esperando una firma o la causa raíz. Se identifica cuándo se tuvo efectivamente constancia con hechos y evaluación inicial; si una reconstrucción demuestra un momento anterior, se corrige con historial y se reevalúa el plazo.

Comunicación del artículo 23.4	Regla de referencia
Alerta temprana	Sin demora indebida y como máximo 24 horas desde la constancia del incidente significativo
Notificación de la letra b	Sin demora indebida y como máximo 72 horas desde esa misma constancia, en el régimen general
Informe intermedio	A solicitud del CSIRT o autoridad competente
Informe final	Como máximo un mes desde la presentación de la notificación de la letra b
Si el incidente continúa en curso en ese hito	Informe de situación entonces y final dentro de un mes desde que se haya gestionado el incidente

Para los prestadores de servicios de confianza, respecto de incidentes significativos que afecten a esos servicios, la notificación de la letra b tiene la excepción de 24 horas. La regla general de 72 no se aplica automáticamente. Los máximos no autorizan a esperar sin necesidad; las ventanas en horas no se convierten en días laborables. [F1]

La alerta indica, cuando proceda, sospecha de actuación ilícita o malintencionada y posibles repercusiones transfronterizas. La notificación añade evaluación inicial de gravedad e impacto e indicadores de compromiso cuando estén disponibles. Si no se conocen indicadores, se explica: no se inventan para completar el formulario.

5. Supuesto adicional C3-NOT-01

Se ha definido para el ejercicio un servicio gestionado adicional SVC-C3-01, separado de SYS-003 y T10-014. Se asume expresamente la aplicabilidad del régimen del artículo 23 y del artículo 10 del Reglamento; no es un servicio de confianza. Son premisas de simulación, no una conclusión sobre la empresa canónica.

Todas las horas son UTC. El servicio queda completamente indisponible desde las 08:55 del 03/11/2026. La primera señal se conoce a las 09:10 y, en las premisas del ejercicio, a las 09:30 se dispone por primera vez del contraste suficiente: 35 minutos de indisponibilidad completa, todavía en curso. Ese es T_constancia del supuesto.

La alerta simulada se envía a las 10:00; el servicio se recupera a las 10:10; la notificación de la letra b se presenta a las 14:00 del mismo día. No se han enviado mensajes reales. Los máximos resultan: alerta el 04/11 a las 09:30 y notificación general el 06/11 a las 09:30. El mes del informe final se referencia a la notificación presentada el 03/11. La fecha de referencia mensual es el 03/12, sujeta al cómputo y calendario aplicables. Las 14:00 UTC de ese día se utilizan como agenda interna conservadora para preparar y remitir el informe; no constituyen una hora límite legal universal. El incidente duró 75 minutos; restablecer el servicio no completa por sí solo su expediente.

El ejemplo completo y sus justificantes ficticios están en los modelos. Si aparecieran datos de constancia anterior, no se conservaría una hora más favorable solo porque ya esté escrita.

6. Rutas paralelas y datos pendientes

La notificación NIS2 se distingue de una eventual comunicación de protección de datos, una obligación del AI Act, avisos a destinatarios de servicios y compromisos contractuales. Cada ruta requiere sujeto y rol, hecho activador, destinatario, momento propio de conocimiento y plazo pertinente. Una notificación no sustituye automáticamente las demás.

El formulario F05 mantiene esa separación. Si hay posible exposición de datos personales, se identifica responsable o encargado y se consulta al DPD cuando corresponda. Si se analiza el AI Act, se comprueban clasificación del sistema, rol, disposición y régimen temporal aplicables. No se aplica un mismo plazo a todo fallo de IA.

T10-014 conserva causa, daño, categoría jurídica y obligación de comunicación sin establecer. Tampoco se afirma una versión implicada sin soporte. El aprendizaje de C3-NOT-01 no sirve para completar esos hechos retrospectivamente.

Actividad 1. La alerta no reinicia las 72 horas

Enunciado: una persona calcula la notificación desde la alerta de las 10:00 del supuesto y propone esperar hasta ese nuevo máximo.

Qué. Corregir el cálculo desde T_constancia a las 09:30 y actuar sin demora indebida.

Por qué. Ambos relojes parten de la misma constancia; el envío de la alerta no abre otras 72 horas.

Cómo. Conservar fundamento y zona horaria, recalcular máximos, preparar contenido conocido y registrar remisión y justificante.

Cuándo. Al activar el procedimiento y en cada revisión de la cronología.

Dónde. En H07 e INC-001.

Con qué. Ficha de aplicabilidad, cronología, procedimiento y canal autorizado; el ejercicio utiliza un canal simulado.

Actividad 2. Notificar con información inicial

Enunciado: ya existe un criterio suficiente de significatividad, pero la causa sigue en investigación; se propone esperar al informe forense completo.

Qué. Comunicar lo exigible con los hechos disponibles y planificar la actualización.

Por qué. La obligación y el reloj no dependen necesariamente de disponer de causa definitiva.

Cómo. Distinguir hechos, sospechas y pendientes; informar según el contenido correspondiente; preservar evidencia y continuar investigación y protección.

Cuándo. Sin demora indebida y dentro del máximo aplicable.

Dónde. En el expediente y canal oficial que corresponda, conservando copia y justificante.

Con qué. Evaluación inicial, responsable y suplente, asesoría y evidencia disponible.

Comprueba lo aprendido

1. ¿Todo error de IA tiene una ventana de 24 horas? No.
2. ¿La notificación general empieza después de la alerta? No.
3. ¿Un mes equivale siempre a 30 días? No.
4. ¿Es necesario acreditar un ataque para toda significatividad? No.

Evidencia de salida

Completa F01-F05 de H07 con el supuesto o un caso autorizado sin información sensible. Deben poder reconstruirse criterio, constancia, destinatario, contenido, máximos y envíos. Una ruta pendiente debe tener comprobación, responsable y siguiente revisión; no un silencio indefinido.

Fuentes

F1. NIS2: artículos 6, 20, 21 y 23.

F2. Reglamento 2024/2690: ámbito y criterios.

F3. NIST CSF 2.0, para organizar la respuesta y recuperación. La correspondencia con el SGIA se concreta por áreas y registros, no por equivalencia literal.

CURSO SGIA · MONOGRÁFICO 3

Responder y comunicar con fundamento

NIS2 + NIST CSF 2.0 · Lección 7

01 Hechos e hipótesis en INC-001

Preserva contexto y evidencia mientras proteges. La causa definitiva puede seguir pendiente.

02 Significatividad según régimen aplicable

No existe un porcentaje único de fallos de IA. Comprueba entidad, servicio y criterios.

03 24 h / 72 h desde la misma constancia

En régimen general, ambos máximos parten de la constancia del incidente significativo.

04 Excepciones, actualizaciones y justificantes

Servicios de confianza tienen excepción. Conserva contenido, envíos y revisiones.

TU EVIDENCIA DE SALIDA

H07: criterio, reloj, destinatario y evidencia

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 7. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Lección 8. Recuperar el servicio y comprobar la mejora

Monográfico 3 · NIS2 y NIST CSF 2.0 · José Manuel Hernández Agudo

Qué aprenderás

Definir objetivos de recuperación, ensayar una alternativa, comprobar el servicio recuperado y preparar decisiones de dirección sobre las mejoras. Trabajo orientativo: 120 minutos, incluida la revisión final.

1. Recuperar la capacidad de prestar el servicio

Restaurar un archivo no demuestra por sí solo que el servicio pueda utilizarse. Pueden faltar permisos, dependencias, datos recientes, registros, supervisión o una configuración segura. La recuperación debe permitir decidir si el servicio funciona dentro de los límites que necesita la organización.

NIS2 contempla continuidad, copias de seguridad, recuperación y crisis, y evaluación de la eficacia de las medidas. El CSF conecta recuperación con el gobierno y las demás funciones. En el SGIA, volver a utilizar una IA requiere considerar su finalidad, riesgos, impactos, supervisión y autorización. [F1, F2]

Se definen antes del ensayo el alcance y los criterios. Si se elige el objetivo después de ver el resultado, la prueba pierde valor para evaluar la preparación.

2. Dos objetivos distintos: tiempo y datos

El **RTO** expresa el objetivo de tiempo para recuperar la capacidad definida. Debe aclarar desde qué hito se mide y qué condiciones permiten dar el servicio por recuperado. El **RPO** expresa el objetivo de punto de recuperación de datos: cuánta antigüedad de datos se admite respecto del hito de referencia. Son objetivos internos que se justifican por el servicio y sus requisitos; no cifras universales de NIS2.

Una prueba puede cumplir el tiempo y no cumplir el punto de datos. También puede restaurar datos recientes en un entorno que todavía no permite operar con seguridad. Por eso se mantienen criterios separados.

Criterio	Pregunta de comprobación
Tiempo	¿Cuándo comenzó el cómputo y cuándo se cumplieron las condiciones de recuperación?
Datos	¿Qué punto se recuperó y qué quedó pendiente de reconstruir o verificar?
Integridad y configuración	¿Lo restaurado corresponde a la referencia adecuada y se ha comprobado?
Seguridad y accesos	¿Se retiró la exposición y se conservan los permisos necesarios?
Función y supervisión	¿La operación y la revisión humana pueden realizarse?
Autorización	¿Existe la decisión necesaria para retomar ese uso y versión?

La cantidad de registros perdidos no se deduce automáticamente de la antigüedad del punto restaurado. Puede existir otra fuente recuperable; hay que comprobarla. Tampoco se afirma que los datos antiguos sean válidos únicamente porque la restauración terminó sin errores.

3. Supuesto adicional C3-REC-01

Se crea un servicio adicional de ensayo, separado de SYS-003 y T10-014. Los objetivos internos fijados antes del ejercicio son RTO de dos horas y RPO de quince minutos. Se incluyen en la recuperación las comprobaciones funcionales y de seguridad necesarias para el uso definido.

El hito inicial es las 09:00. La restauración técnica termina a las 10:35 y las comprobaciones concluyen a las 10:50. El último punto de datos restaurado y verificado corresponde a las 08:40; no se aporta evidencia de reconstrucción posterior.

Resultado	Cálculo	Conclusión del ejercicio
Restauración técnica	95 minutos desde las 09:00	Hito técnico, todavía sin completar todas las comprobaciones
Recuperación con las comprobaciones definidas	110 minutos	Cumple el objetivo interno de 120 minutos del supuesto
Antigüedad del punto recuperado	20 minutos respecto de las 09:00	Supera los 15 minutos admitidos: no cumple ese objetivo de punto

No se comunica «recuperación conforme» ocultando el segundo resultado. La autoridad debe conocer la carencia, su efecto y las opciones. El ejemplo no acredita un daño real ni un número concreto de registros irrecuperables. Se propone comprobar fuentes adicionales y mejorar el mecanismo pertinente antes de repetir la prueba.

4. Ensayar sin agravar el riesgo

El ensayo identifica entorno, autorización, responsables, datos, dependencias, medidas de protección y condiciones de interrupción. Se evita que una prueba de recuperación sobrescriba evidencia necesaria o altere un servicio real sin control. Cuando se necesitan datos representativos se justifica su uso y protección.

Las copias se evalúan como parte de un sistema de recuperación: qué contienen, quién puede modificarlas, cómo se accede, si se dispone de las claves necesarias y qué dependencia podría impedir utilizarlas. «Copia completada» y «restauración comprobada» son evidencias distintas.

Una alternativa manual también necesita prueba. Se examinan capacidad, información disponible, competencias, duración sostenible y riesgos para las personas. El simple enunciado «volvemos a proceso manual» no demuestra que pueda absorberse el trabajo ni mantenerse la supervisión necesaria.

5. Decidir la vuelta al servicio

El responsable prepara resultados y carencias; la autoridad correspondiente decide según los requisitos y límites. Puede ser necesario mantener una restricción, utilizar una alternativa o completar comprobaciones. Las condiciones de una decisión temporal deben ser concretas, revisables y compatibles con las obligaciones aplicables.

Para SYS-003, no se supone que v2 estuviera desplegada. Su estado sigue siendo **probada, sin autorización de despliegue**. Una recuperación hipotética o un proveedor disponible no crea esa autorización. Tampoco se autoriza v1 por detectar más críticos en una muestra.

La vuelta a operación no equivale siempre al cierre del incidente. Pueden quedar investigación, comunicaciones, mejoras o comprobaciones pendientes. INC-001 distingue esos estados y sus fuentes, sin generar copias contradictorias en el tablero.

6. Comprobar la eficacia de una mejora

Una acción puede haberse ejecutado sin resolver el problema. Si la carencia era la pérdida de avisos a guardia, cambiar una regla o contratar una plataforma no demuestra que ahora se reciben. La eficacia se comprueba con un ensayo o evidencia pertinente, con alcance y criterio definidos.

En C3-DET-01 se observaban nueve registros, ocho alertas y siete avisos recibidos de diez eventos previstos. Una nueva prueba debe identificar condiciones, eventos y resultados por etapa. No se presume que usar otra muestra permita una comparación causal perfecta. Se explica qué sostiene el ensayo y qué queda fuera.

La revisión final relaciona medidas con riesgos e impactos, proveedores, cambios, formación y supervisión. Si una acción no funciona, se revisa el tratamiento; no se cierra por estar vencida o por haber gastado el presupuesto previsto.

7. Qué necesita la dirección al cerrar el ciclo

Un expediente útil presenta: servicio y alcance; objetivos y requisitos; evidencia de la recuperación; incidentes y comunicaciones; carencias y riesgos residuales; decisiones solicitadas; responsables y seguimiento. Las cifras deben acompañarse de límites y pendientes. No basta un panel de colores.

La revisión también considera qué supuestos del plan han dejado de ser válidos. Un nuevo proveedor, un cambio de finalidad o una ampliación de permisos puede exigir actualizar mapas, perfiles y pruebas. La mejora conecta de nuevo con las primeras lecciones del monográfico.

Actividad 1. Corregir un cierre prematuro

Enunciado: se marca C3-REC-01 como completamente satisfactorio porque la restauración técnica tardó 95 minutos.

Qué. Informar por separado recuperación comprobada y punto de datos, manteniendo abierta la carencia del RPO.

Por qué. El hito técnico no incluía todas las condiciones, y el punto recuperado excede el objetivo interno.

Cómo. Mostrar 110 minutos y 20 minutos con referencias, examinar efecto y alternativas y preparar una mejora con prueba posterior.

Cuándo. Antes de cerrar el ensayo o presentar el resultado a dirección.

Dónde. En H08, con enlaces a continuidad, incidentes y acciones pertinentes.

Con qué. Objetivos previos, marcas temporales, prueba funcional y evidencia del punto de datos.

Actividad 2. Distinguir acción y eficacia

Enunciado: una acción dice «nuevo canal de avisos contratado» y se propone cerrar la pérdida de recepción detectada en la lección 6.

Qué. Mantener pendiente la comprobación de la cadena completa de aviso.

Por qué. La contratación acredita una actuación, pero no que el resultado deseado se haya alcanzado.

Cómo. Preparar ensayo autorizado, observar generación, recepción, triaje y suplencia y comparar con el criterio interno, conservando limitaciones.

Cuándo. Antes de declarar eficaz la medida y cuando un cambio relevante pueda invalidarla.

Dónde. En H06, H08 y los registros de seguimiento y mejora del SGIA.

Con qué. Eventos sintéticos, registros y justificantes de recepción, responsables y criterios previos.

Comprueba lo aprendido

1. ¿Restaurar un archivo equivale a recuperar un servicio? No.
2. ¿Los objetivos de RTO y RPO son mínimos universales de NIS2? No.
3. ¿Cumplir el tiempo permite ocultar un incumplimiento del punto de datos? No.
4. ¿Servicio restablecido significa siempre incidente cerrado? No.

Evidencia de salida

Completa H08 con objetivos previos, ensayo, resultados y propuesta de decisión. Resuelve después el caso final del monográfico.

Fuentes

F1. NIS2, artículo 21.2.c y 21.2.f.

F2. NIST CSF 2.0.

F3. ENISA: guía técnica de implementación. Los objetivos y resultados de C3-REC-01 son supuestos docentes internos.

Clase de audio 047

047. NIS2 y NIST CSF 2.0: detección, notificación y recuperación

Claves para aplicar esta clase

Utiliza estas cinco claves al resolver los ejercicios de detección, notificación y recuperación:

1. **Detección y mejora.** Los resultados 9/10, 8/10 y 7/10 describen las etapas del ensayo; no acreditan una reparación ni cobertura general. Los eventos son sintéticos y no ataques reales. Para medir latencia se necesitan marcas de inicio y fin; recibir un aviso no demuestra una actuación humana. Las pérdidas de la cadena siguen pendientes de investigación y comprobación, sin asignar tiempo cero a lo que no llegó.

2. **Ámbito y umbral.** El artículo 10.a del Reglamento 2024/2690 exige indisponibilidad completa que supere treinta minutos, dentro de su ámbito. Treinta minutos exactos no cumplen por sí solos esa letra; se revisan los demás criterios aplicables. El caso supera ese umbral con treinta y cinco minutos a las 09:30 UTC. Esa constancia es una premisa del ejercicio y no permite demorar un conocimiento que en otro caso fuera anterior.

3. **Comunicaciones.** Las 24 y 72 horas generales parten de la misma constancia y se actúa sin demora indebida. Para los servicios de confianza, la excepción de 24 horas afecta a la notificación de la letra b. El mes ordinario del informe final parte de la notificación presentada. Si el incidente continúa en curso, se presenta situación en el hito correspondiente y el final como máximo un mes después de haberlo gestionado. No se espera indefinidamente al cierre administrativo. Las 14:00 del 3 de diciembre son agenda interna para preparar y remitir el informe, no un límite jurídico universal.

4. **Recuperación y datos.** El tercer ejercicio comienza a las 09:00. Los 110 minutos de recuperación comprobada cumplen el RTO interno de 120; el punto de las 08:40 tiene veinte minutos de antigüedad y supera el RPO interno de quince. No se demuestra por ello pérdida irreversible, cantidad de registros afectados ni daño. La reconstrucción posterior y la autorización de retorno necesitan su propia evidencia y decisión.

5. **Integración con el SGIA.** ISO/IEC 42001 es una norma de sistema de gestión de IA, vinculada a responsabilidades, riesgos e impactos, operación, evaluación y mejora. Sus conexiones con NIS2 y NIST CSF son funcionales. Mantén separados los tres ejercicios, sus cronologías y sus evidencias; enlaza seguimiento, incidentes y cambios sin crear estados contradictorios.

Referencias: Reglamento 2024/2690, artículo 10; NIS2, artículo 23.4; ISO/IEC 42001:2023.

CURSO SGIA · MONOGRÁFICO 3

Recuperar y demostrar la mejora

NIS2 + NIST CSF 2.0 · Lección 8

01 Objetivos de tiempo y datos definidos

RTO y RPO son objetivos distintos. Justifica hitos y condiciones antes del ensayo.

02 Restauración y servicio comprobados

Terminar una restauración técnica no prueba que el servicio pueda utilizarse con seguridad.

03 Decisión con carencias y límites

El supuesto cumple tiempo de 120 minutos, pero no el punto de datos objetivo de 15.

04 Acción realizada y eficacia verificadas

Una acción realizada no equivale a mejora eficaz. Comprueba el resultado que faltaba.

TU EVIDENCIA DE SALIDA

H08: 110 minutos y punto de datos de 20 minutos

José Manuel Hernández Agudo
Seguridad de los sistemas de IA

Lección 8. Mi aplicación al servicio

Completa con hechos, evidencias, límites y decisiones identificadas.

Qué concluyo y con qué fundamento

Cómo lo aplico: hechos, fuentes y límites

Qué debo comprobar, quién lo hará y cuándo

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Alcance y aplicabilidad

C3-H01 · José Manuel Hernández Agudo · 25/10/2026

Finalidad

Delimitar la entidad, el servicio, los sistemas y los usos y documentar el fundamento de cada obligación antes de declarar cumplimiento.

Conexión con el SGIA

Gobierno, contexto y responsabilidades del SGIA. Reutiliza registros y localizadores existentes; identifica la fuente autorizada de cada dato y conserva las revisiones.

Campos de la ficha

1. **Entidad y servicio:** [Completar con evidencia o pendiente justificado].
2. **Sistema, uso, versión y entorno:** [Completar con evidencia o pendiente justificado].
3. **Actividad, tamaño y reglas específicas examinadas:** [Completar con evidencia o pendiente justificado].
4. **Jurisdicción y disposiciones aplicables:** [Completar con evidencia o pendiente justificado].
5. **Fuente oficial, versión y fecha:** [Completar con evidencia o pendiente justificado].
6. **Conclusión y límites de aplicabilidad:** [Completar con evidencia o pendiente justificado].
7. **Fuente autorizada del estado:** [Completar con evidencia o pendiente justificado].
8. **Responsables, suplencias y RACI:** [Completar con evidencia o pendiente justificado].
9. **Pendientes y siguiente comprobación:** [Completar con evidencia o pendiente justificado].

Cómo trabajarla

Primero delimita el alcance y distingue hechos, propuestas y datos pendientes. Consulta las fuentes y registros pertinentes. Completa la ficha sin copiar secretos ni datos personales innecesarios. Vincula la evidencia que sostiene cada conclusión y asigna responsable y siguiente paso a las carencias. Una propuesta no se registra como actuación realizada ni como decisión autorizada.

Modelo del ejercicio

Los datos siguientes son didácticos; los supuestos adicionales no acreditan implantación ni incidentes reales en la empresa ficticia.

Campo	Respuesta orientativa
Entidad y servicio	Tech Server IIT Spain, ficticia; alcance de evaluación
Sistema, uso, versión y entorno	SYS-003 / USO-004 / v2; entorno de evaluación del supuesto C3-ALC-01
Actividad, tamaño y reglas específicas examinadas	Actividad y tamaño no establecidos suficientemente en el caso
Jurisdicción y disposiciones aplicables	Determinar mediante análisis documentado; no inferir de la ubicación nominal
Fuente oficial, versión y fecha	Directiva (UE) 2022/2555 y fuentes pertinentes, consulta 25/10/2026

Campo	Respuesta orientativa
Conclusión y límites de aplicabilidad	Aplicabilidad concreta pendiente; preparar comprobaciones mientras se delimita
Fuente autorizada del estado	v2 probada, sin autorización de despliegue; identificar expediente autorizado sin inventar localizador
Responsables, suplencias y RACI	RACI C3-H01A propuesta; titulares y delegaciones por confirmar
Pendientes y siguiente comprobación	Obtener datos de actividad, tamaño y servicio y revisar régimen pertinente

Antes de cerrar

La conclusión debe poder seguirse desde los hechos hasta las fuentes. Un pendiente tiene responsable y comprobación; no se convierte en no aplicable.

La persona revisora debe poder reconstruir alcance, evidencia, límites, responsable y decisión. Se mantienen las autorizaciones del caso; v2 de SYS-003 sigue probada, sin autorización de despliegue.

Responsabilidades y formación para gobernar la seguridad de la IA

C3-H01A · Anexo de la ficha de alcance · Lección 1

José Manuel Hernández Agudo · Monográfico 3 · 25/10/2026

Para qué sirve

Esta plantilla permite asignar quién prepara, ejecuta, decide y recibe información sobre las medidas de seguridad de un servicio que utiliza IA. Se completa después de delimitar entidad, servicio, sistemas, usos y versiones. El resultado debe incluir responsables confirmados, suplencias, autoridad suficiente y evidencias de que las tareas se realizan.

El órgano de dirección necesita poder explicar qué medidas ha aprobado, cómo supervisa su ejecución y qué hace ante las carencias. Designar un AIO o un CISO ayuda a organizar el trabajo. Esa designación no extingue la responsabilidad que corresponda al órgano de dirección.

1. Separar la obligación y la organización interna

El artículo 20.1 de NIS2 establece que los Estados miembros deben asegurar que los órganos de dirección de las entidades esenciales e importantes aprueben las medidas adoptadas para cumplir el artículo 21, supervisen su puesta en práctica y respondan por el incumplimiento de ese artículo por la entidad. La concreción jurídica requiere considerar el régimen nacional aplicable; una matriz RACI no determina por sí misma responsabilidades civiles, administrativas o penales. [F1]

En una sociedad puede intervenir el Consejo de Administración; en otra estructura habrá que identificar el órgano de dirección que corresponda. No se presupone que todas las entidades tengan un consejo.

AIO - AI Officer: denominación interna propuesta para coordinar el gobierno de IA y el SGIA. **CISO:** función propuesta para coordinar la seguridad de la información y la respuesta técnica. El artículo 20 no crea por sí solo cargos obligatorios con esos nombres ni una transferencia de responsabilidad hacia ellos.

Un AIO conecta finalidad, riesgos e impactos de IA, supervisión, cambios y autorizaciones. El CISO conecta amenazas, medidas de seguridad, detección, respuesta y recuperación. El propietario del servicio responde de su operación dentro de la autoridad asignada. Deben trabajar sobre un expediente común y conservar las decisiones que correspondan a cada función.

2. Cabecera que debes cumplimentar

Campo	Respuesta
Identificador y versión de la matriz	[Completar]
Entidad y órgano de dirección identificado	[Completar]
Servicio, sistema y uso	[Completar]
Versión y entorno incluidos	[Completar]
Fuente del estado de autorización	[Localizador del registro autorizado]
Fundamento de aplicabilidad NIS2 y normativa nacional	[Fuente, fecha y razonamiento; indicar pendientes]
Roles reales, titulares y suplentes	[Completar en registro de acceso restringido]
Límites de delegación y medidas urgentes autorizadas	[Completar]
Canal ordinario y canal de emergencia	[Completar y probar]
Aprobación, revisión y próxima comprobación	[Completar con evidencia; no anticipar firmas]

3. Cómo leer la RACI

- **R - Realiza:** prepara o ejecuta la actividad y aporta la evidencia.
- **A - Decide y responde internamente por esa tarea:** tiene autoridad para aprobar su resultado dentro de los límites asignados.
- **C - Consultado:** aporta criterio antes de decidir o ejecutar.
- **I - Informado:** recibe la información pertinente.
- **A/R:** una misma función decide y ejecuta esa tarea.

Como criterio de diseño de esta plantilla se asigna una sola A por fila y al menos una R. Puede haber varias personas ejecutoras. La A de una tarea operativa no sustituye las responsabilidades legales que puedan corresponder a otras funciones.

Abreviaturas: **OD**, órgano de dirección; **DG**, dirección ejecutiva delegada; **AIO**, coordinación del SGIA; **CISO**, seguridad; **OPS**, propietario del servicio y equipo de operación; **JUR**, asesoría jurídica; **PERSONAS**, formación y gestión de personas; **COMPRAS**, contratación. Cuando haya datos personales se consulta además al DPD, si está designado, preservando su independencia. El DPD no se convierte en el responsable de cumplir por la entidad.

4. Modelo propuesto de asignación

Este modelo es una propuesta didáctica. Los titulares y las delegaciones deben confirmarse antes de utilizarlo en una organización.

01. Preparar el análisis de aplicabilidad y el alcance

OD: I · **DG:** A · **AIO:** R · **CISO:** C · **OPS:** C · **JUR:** R · **PERSONAS:** - · **COMPRAS:** C

02. Aprobar medidas de gestión de riesgos del art. 21

OD: A · **DG:** R · **AIO:** C · **CISO:** R · **OPS:** C · **JUR:** C · **PERSONAS:** C · **COMPRAS:** C

03. Supervisar su ejecución y resolver desviaciones relevantes

OD: A · **DG:** R · **AIO:** R · **CISO:** R · **OPS:** C · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

04. Dotar recursos para las medidas aprobadas

OD: A · **DG:** R · **AIO:** C · **CISO:** C · **OPS:** C · **JUR:** - · **PERSONAS:** C · **COMPRAS:** C

05. Mantener riesgos, impactos y decisiones de uso de IA

OD: I · **DG:** A · **AIO:** R · **CISO:** C · **OPS:** R · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

06. Diseñar y comprobar las medidas técnicas de seguridad

OD: I · **DG:** A · **AIO:** C · **CISO:** R · **OPS:** R · **JUR:** C · **PERSONAS:** - · **COMPRAS:** C

07. Autorizar un cambio o despliegue de IA dentro de la delegación

OD: I · **DG:** A · **AIO:** R · **CISO:** C · **OPS:** R · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

08. Evaluar al proveedor y documentar carencias

OD: I · **DG:** A · **AIO:** R · **CISO:** R · **OPS:** C · **JUR:** C · **PERSONAS:** - · **COMPRAS:** R

09. Formalizar requisitos y obligaciones contractuales

OD: I · **DG:** A · **AIO:** C · **CISO:** C · **OPS:** C · **JUR:** R · **PERSONAS:** - · **COMPRAS:** R

10. Detectar, registrar y realizar el triaje de señales

OD: I · **DG:** I · **AIO:** C · **CISO:** A · **OPS:** R · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

11. Ejecutar contención y recuperación dentro de lo autorizado

OD: I · **DG:** I · **AIO:** C · **CISO:** A · **OPS:** R · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

12. Evaluar la significatividad y la obligación de comunicar

OD: I · **DG:** A · **AIO:** C · **CISO:** R · **OPS:** R · **JUR:** R · **PERSONAS:** - · **COMPRAS:** -

13. Remitir comunicaciones oficiales y conservar justificantes

OD: I · **DG:** A · **AIO:** C · **CISO:** R · **OPS:** C · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

14. Completar la formación de los miembros del órgano de dirección

OD: A/R · **DG:** C · **AIO:** C · **CISO:** C · **OPS:** - · **JUR:** C · **PERSONAS:** R · **COMPRAS:** -

15. Ejecutar y documentar el plan de formación por funciones

OD: I · **DG:** A · **AIO:** R · **CISO:** R · **OPS:** C · **JUR:** C · **PERSONAS:** R · **COMPRAS:** -

16. Revisar la eficacia y aprobar mejoras relevantes

OD: A · **DG:** R · **AIO:** R · **CISO:** R · **OPS:** C · **JUR:** C · **PERSONAS:** - · **COMPRAS:** -

Las filas 10 y 11 necesitan una delegación previa que describa límites de contención, parada, reversión y preservación de evidencia. La fila 13 necesita un remitente autorizado y un suplente con acceso al canal

oficial. No se espera una reunión del consejo para realizar una notificación que ya resulte exigible.

Si una persona acumula AIO, CISO y operación, se identifican los conflictos y se dispone revisión adicional de las decisiones relevantes. Cambiar el nombre del cargo no resuelve la falta de medios o de independencia en una comprobación.

5. Formación de dirección: dos fundamentos que deben quedar claros

Ciberseguridad - artículo 20.2 NIS2. La Directiva prevé asistencia a formación de los miembros de los órganos de dirección de las entidades esenciales e importantes. Busca que puedan identificar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios. También prevé que se aliente formación similar y periódica para empleados. El artículo 21.2.g incluye ciberhigiene y formación dentro de las medidas de gestión de riesgos. [F1]

IA - artículo 4 del AI Act y competencias del SGIA. Se documentan por separado las medidas de alfabetización en IA que correspondan al proveedor o responsable del despliegue y las competencias que requieren las funciones asignadas. El artículo 4, en su redacción modificada en 2026, exige medidas de apoyo a la alfabetización del personal y de quienes operan o utilizan sistemas por cuenta de la organización, atendiendo a su contexto; no impone garantizar un nivel específico de cada persona. No crea un curso idéntico ni una certificación obligatoria para todo consejero por el mero hecho de serlo. [F2]

En este modelo se propone que quienes gobiernan decisiones de IA reciban formación sobre sus riesgos, límites y evidencias. Se puede establecer como requisito interno del cargo, con su aprobación y registro. No se atribuye esa decisión interna al artículo 20 de NIS2.

Programa directivo propuesto

Las duraciones siguientes son una propuesta docente de la organización, no mínimos legales.

Bloque	Duración propuesta	Capacidad que se debe demostrar	Evidencia práctica
Gobierno de ciberseguridad	2 horas	Identificar qué aprueba y supervisa la dirección; priorizar un riesgo del servicio	Decisión razonada sobre riesgo, recursos y seguimiento
Gobierno de IA	2 horas	Distinguir calidad, seguridad e impactos; interpretar métricas y estados de autorización	Caso SYS-003: explicar por qué 94/100 no autoriza v2
Ejercicio de incidente	1 hora	Activar suplencias, analizar destinatarios y reconstruir los relojes	Cronología y borrador de alerta del supuesto C3-NOT-01

La revisión anual, la formación al incorporarse al cargo y la actualización ante cambios relevantes se proponen como reglas internas. Su frecuencia se adapta a necesidades, riesgos y requisitos aplicables. Un certificado de asistencia acredita asistencia; la capacidad para decidir se comprueba mediante una actividad pertinente y sus resultados.

Ficha de competencia y formación

Persona o función: [Completar]. Responsabilidad: [Completar]. Necesidad detectada: [Completar]. Fundamento: [NIS2 / alfabetización IA / competencia SGIA / requisito interno]. Actividad y fecha: [Completar]. Evidencia de asistencia: [Localizador]. Ejercicio realizado: [Localizador]. Resultado observado: [Completar]. Carencia y apoyo adicional: [Completar]. Responsable de seguimiento: [Completar]. Próxima revisión: [Completar].

6. Aplicación resuelta a la lección 1

En el supuesto adicional C3-ALC-01, una de dos cuentas administrativas carece de responsable registrado. OPS realiza el inventario y comprueba dependencias; CISO coordina la revisión de accesos; AIO comprueba la relación con el entorno de evaluación y el estado de v2; DG decide las actuaciones dentro de su delegación. OD recibe la información que necesite para supervisar medidas y desviaciones relevantes.

El expediente debe mostrar la revisión y la decisión efectiva. Esta asignación propuesta no demuestra que ya se hayan nombrado esos cargos ni que se hayan aplicado medidas en Tech Server IIT Spain.

La v2 permanece probada, sin autorización de despliegue. La matriz no autoriza v1 por comparación ni convierte una carencia de inventario en un ataque demostrado.

7. Actividad resuelta: «Que lo firme el AIO»

Enunciado hipotético: se propone que el AIO firme un documento aceptando toda la responsabilidad de NIS2 para que el consejo deje de intervenir.

Qué. Rechazar esa sustitución y preparar una asignación de tareas y autoridad verificable.

Por qué. La distribución interna del trabajo no elimina las responsabilidades que la legislación atribuya al órgano de dirección.

Cómo. Identificar el órgano correspondiente y la norma aplicable; conservar aprobación y supervisión en ese nivel; asignar preparación y ejecución a AIO, CISO y operación; documentar delegaciones, suplencias y evidencias.

Cuándo. Al aprobar la estructura de gobierno y antes de utilizar la firma para afirmar cumplimiento.

Dónde. En el expediente de alcance, la RACI, las decisiones de dirección y los registros de formación.

Con qué. Fuentes oficiales, estructura real de la entidad, decisiones de nombramiento, límites de autoridad y registros de seguimiento.

Fuentes y correspondencia

F1. Directiva (UE) 2022/2555, artículos 20 y 21.

F2. Reglamento (UE) 2026/1744, artículo 1.5, que modifica el artículo 4 del AI Act.

F3. NIST CSF 2.0: conexión funcional con gobierno y definición de responsabilidades.

F4. ISO/IEC 42001:2023: liderazgo, responsabilidades, competencia, operación y evaluación del SGIA. La RACI es una herramienta del curso; no se presenta como formulario exigido literalmente por la norma.

Perfil y prioridades

C3-H02 · José Manuel Hernández Agudo · 25/10/2026

Finalidad

Comparar situación acreditada y resultados deseados y preparar un plan de actuaciones priorizado, sin convertir el perfil en una certificación.

Conexión con el SGIA

Riesgos, objetivos, tratamiento y evaluación del SGIA. Reutiliza registros y localizadores existentes; identifica la fuente autorizada de cada dato y conserva las revisiones.

Campos de la ficha

1. **Resultado deseado y alcance:** [Completar con evidencia o pendiente justificado].
2. **Situación actual y evidencia:** [Completar con evidencia o pendiente justificado].
3. **Estado de evaluación:** [Completar con evidencia o pendiente justificado].
4. **Brecha e incertidumbre:** [Completar con evidencia o pendiente justificado].
5. **Prioridad y fundamento:** [Completar con evidencia o pendiente justificado].
6. **Actuación y recursos:** [Completar con evidencia o pendiente justificado].
7. **Responsable y autoridad:** [Completar con evidencia o pendiente justificado].
8. **Fecha o hito:** [Completar con evidencia o pendiente justificado].
9. **Criterio y evidencia de cierre:** [Completar con evidencia o pendiente justificado].

Cómo trabajarla

Primero delimita el alcance y distingue hechos, propuestas y datos pendientes. Consulta las fuentes y registros pertinentes. Completa la ficha sin copiar secretos ni datos personales innecesarios. Vincula la evidencia que sostiene cada conclusión y asigna responsable y siguiente paso a las carencias. Una propuesta no se registra como actuación realizada ni como decisión autorizada.

Modelo del ejercicio

Los datos siguientes son didácticos; los supuestos adicionales no acreditan implantación ni incidentes reales en la empresa ficticia.

Campo	Respuesta orientativa
Resultado deseado y alcance	Atribuir y justificar accesos administrativos del ensayo C3-GOB-01
Situación actual y evidencia	Dos cuentas; una carece de responsable registrado en el supuesto
Estado de evaluación	Parcial
Brecha e incertidumbre	Falta atribución y revisión de necesidad de esa cuenta
Prioridad y fundamento	Primera en el plan propuesto: afecta a trazabilidad del entorno de evaluación
Actuación y recursos	Confirmar uso, permisos y dependencias; decidir medida y comprobar resultado

Campo	Respuesta orientativa
Responsable y autoridad	OPS y CISO realizan; DG decide dentro de delegación propuesta
Fecha o hito	Antes de ampliar el acceso; fijar fecha al aprobar plan
Criterio y evidencia de cierre	Registro y permisos efectivos revisados, decisión y prueba conservadas

Antes de cerrar

El cierre se refiere al resultado y su evidencia. Acreditado, parcial, no evidenciado y no revisado son estados internos de la herramienta.

La persona revisora debe poder reconstruir alcance, evidencia, límites, responsable y decisión. Se mantienen las autorizaciones del caso; v2 de SYS-003 sigue probada, sin autorización de despliegue.

Activos, dependencias y escenarios

C3-H03 · José Manuel Hernández Agudo · 25/10/2026

Finalidad

Reconstruir las relaciones relevantes del servicio y vincular condiciones y escenarios con evidencias y decisiones.

Conexión con el SGIA

Recursos, datos, ciclo de vida, riesgos e impactos. Reutiliza registros y localizadores existentes; identifica la fuente autorizada de cada dato y conserva las revisiones.

Campos de la ficha

1. **Activo o dependencia:** [Completar con evidencia o pendiente justificado].
2. **Servicio y entorno:** [Completar con evidencia o pendiente justificado].
3. **Responsabilidad y fuente del dato:** [Completar con evidencia o pendiente justificado].
4. **Relación, origen y destino:** [Completar con evidencia o pendiente justificado].
5. **Datos o permisos transferidos:** [Completar con evidencia o pendiente justificado].
6. **Condición y escenario:** [Completar con evidencia o pendiente justificado].
7. **Consecuencia posible:** [Completar con evidencia o pendiente justificado].
8. **Evidencia y límites:** [Completar con evidencia o pendiente justificado].
9. **Registro vinculado y comprobación pendiente:** [Completar con evidencia o pendiente justificado].

Cómo trabajarla

Primero delimita el alcance y distingue hechos, propuestas y datos pendientes. Consulta las fuentes y registros pertinentes. Completa la ficha sin copiar secretos ni datos personales innecesarios. Vincula la evidencia que sostiene cada conclusión y asigna responsable y siguiente paso a las carencias. Una propuesta no se registra como actuación realizada ni como decisión autorizada.

Modelo del ejercicio

Los datos siguientes son didácticos; los supuestos adicionales no acreditan implantación ni incidentes reales en la empresa ficticia.

Campo	Respuesta orientativa
Activo o dependencia	Conjunto de tickets sintéticos del supuesto C3-DEP-01
Servicio y entorno	Ensayo aislado; arquitectura adicional expresamente definida
Responsabilidad y fuente del dato	Función de datos y ejecución del ejercicio; no titular real nombrado
Relación, origen y destino	Recepción → versión de entrada → ejecución de evaluación
Datos o permisos transferidos	Contenido sintético y permiso de lectura del ejecutor
Condición y escenario	Confusión de versión de entrada podría invalidar la comparación

Campo	Respuesta orientativa
Consecuencia posible	Conclusión de evaluación basada en un conjunto distinto del identificado
Evidencia y límites	Se requiere manifiesto y protocolo; el ejemplo no acredita que existan en SYS-003
Registro vinculado y comprobación pendiente	FD-001 y CAM-001; comprobar identificador utilizado en la ejecución

Antes de cerrar

No se añade un componente porque resulte útil para explicar una amenaza: debe estar definido o señalarse como hipótesis o supuesto adicional.

La persona revisora debe poder reconstruir alcance, evidencia, límites, responsable y decisión. Se mantienen las autorizaciones del caso; v2 de SYS-003 sigue probada, sin autorización de despliegue.

Protección y pruebas

C3-H04 · José Manuel Hernández Agudo · 25/10/2026

Finalidad

Distinguir diseño, ejecución, observación y decisión para demostrar el resultado pertinente de una medida.

Conexión con el SGIA

Operación, datos, recursos, cambios y tratamiento del riesgo. Reutiliza registros y localizadores existentes; identifica la fuente autorizada de cada dato y conserva las revisiones.

Campos de la ficha

1. **Riesgo y alcance:** [Completar con evidencia o pendiente justificado].
2. **Medida y fundamento:** [Completar con evidencia o pendiente justificado].
3. **Configuración o referencia:** [Completar con evidencia o pendiente justificado].
4. **Criterio previo de aceptación:** [Completar con evidencia o pendiente justificado].
5. **Ensayo autorizado y límites:** [Completar con evidencia o pendiente justificado].
6. **Resultado observado:** [Completar con evidencia o pendiente justificado].
7. **Carencia o incertidumbre:** [Completar con evidencia o pendiente justificado].
8. **Decisión y autoridad:** [Completar con evidencia o pendiente justificado].
9. **Evidencia y próxima revisión:** [Completar con evidencia o pendiente justificado].

Cómo trabajarla

Primero delimita el alcance y distingue hechos, propuestas y datos pendientes. Consulta las fuentes y registros pertinentes. Completa la ficha sin copiar secretos ni datos personales innecesarios. Vincula la evidencia que sostiene cada conclusión y asigna responsable y siguiente paso a las carencias. Una propuesta no se registra como actuación realizada ni como decisión autorizada.

Modelo del ejercicio

Los datos siguientes son didácticos; los supuestos adicionales no acreditan implantación ni incidentes reales en la empresa ficticia.

Campo	Respuesta orientativa
Riesgo y alcance	C3-PRO-01, clave ficticia de integración de ensayo
Medida y fundamento	Revocar clave y comprobar alternativa autorizada
Configuración o referencia	Referencia de clave sin valor secreto; entorno con datos sintéticos
Criterio previo de aceptación	La clave revocada no permite llamadas y la alternativa conserva la operación definida
Ensayo autorizado y límites	Operaciones controladas antes y después; no usar producción ni credenciales reales

Campo	Respuesta orientativa
Resultado observado	Resultado que debe cumplimentarse al realizar el ensayo; no se inventa una prueba ejecutada
Carencia o incertidumbre	Comprobar posibles sesiones o credenciales distintas si el rechazo no se observa
Decisión y autoridad	Pendiente hasta contar con resultado y autoridad identificada
Evidencia y próxima revisión	Localizar configuración y salidas de prueba; mantener secretos fuera de la ficha

Antes de cerrar

Una captura de configuración no acredita por sí sola eficacia; una propuesta de prueba no se marca como ejecutada.

La persona revisora debe poder reconstruir alcance, evidencia, límites, responsable y decisión. Se mantienen las autorizaciones del caso; v2 de SYS-003 sigue probada, sin autorización de despliegue.

Evaluación rápida de proveedores y componentes de IA

C3-H05 · Cuestionario y decisión de uso · Herramienta para la lección 5

José Manuel Hernández Agudo · Monográfico 3 · 25/10/2026

1. Qué decisión ayuda a preparar

El cuestionario permite revisar un proveedor de API, un servicio de ajuste de modelos -fine-tuning- o un modelo de terceros antes de incorporarlo a un uso concreto. También permite reevaluar cambios. Se adapta a lo que se adquiere y al riesgo del servicio; un modelo descargado y una API remota tienen dependencias diferentes.

La evaluación reúne información comercial, contractual y técnica, y la relaciona con pruebas propias. Su resultado se incorpora a **PROV-001** y a los expedientes vinculados; no reemplaza la evaluación de riesgos ni la autorización del sistema o de su despliegue.

El cuestionario es una herramienta original del curso. Utiliza **GV.SC** del NIST CSF 2.0 para ordenar la revisión de la cadena de suministro. La conexión principal en ISO/IEC 42001 es **A.10, relaciones con terceros y clientes**. **A.7, datos para sistemas de IA**, añade las comprobaciones sobre datos. A.7 no representa por sí sola todo el gobierno de proveedores. [F1-F3]

2. Cabecera y criticidad

Completa: identificador de evaluación; entidad; proveedor y servicio exactos; contrato y versión; fecha; propietario del servicio; AIO, CISO y Compras participantes; uso y finalidad; entorno; datos que saldrán de la organización; ubicaciones; subproveedores conocidos; dependencias de continuidad; posibilidad de sustituir el componente; versión del modelo y configuración cuando corresponda; estado de autorización y fuente que lo acredita.

La criticidad debe justificarse por el efecto de la dependencia, los datos, permisos y posibilidades de recuperación. No se deduce únicamente de la marca, el precio o la categoría «IA». Cuando se cambien datos, permisos, ubicación, modelo, proveedor o finalidad, se revisa el alcance de la evaluación.

3. Respuestas que se aceptan

Para cada pregunta registra **respuesta**, **evidencia y versión**, **comprobación propia**, **conclusión**, **carencia**, **acción**, **responsable**, **fecha objetivo** y **verificación de cierre**.

- **Suficiente:** la evidencia y las comprobaciones sostienen el criterio para el alcance examinado.
- **Parcial:** existe información útil, pero falta una parte necesaria o la prueba solo cubre parte del alcance.
- **No evidenciado:** no se dispone de evidencia suficiente; no significa automáticamente que el proveedor carezca del control.
- **No aplica:** se justifica por qué la pregunta no corresponde al servicio o uso. No se utiliza como sustituto de «no sabemos».

Una declaración comercial, un documento contractual y una prueba técnica aportan evidencias de naturaleza distinta. Si se aporta una certificación, se comprueban emisor, vigencia, alcance y límites. No se presenta como aval de NIST ni como prueba de la seguridad completa de la integración.

4. Las veinte preguntas

La columna GV.SC indica la conexión de trabajo propuesta por el curso. No declara una correspondencia oficial ni exhaustiva con cada subcategoría del CSF. Los ejemplos de evidencia se ajustan a la modalidad y al riesgo.

ID	Pregunta	Evidencia y comprobación sugeridas	GV.SC
Q01	¿Quién gobierna esta dependencia y qué política y proceso se aplican a su contratación y revisión?	Política o procedimiento propio; responsable confirmado; expediente de la evaluación	01
Q02	¿Cómo se reparten las responsabilidades entre nuestra organización, proveedor y otros terceros?	Acuerdo de responsabilidades; contactos y suplentes; contraste con el servicio adquirido	02
Q03	¿Qué riesgos de esta dependencia se han vinculado al servicio y al SGIA?	Escenarios en R-001 e IMP-001; tratamiento, decisión y seguimiento	03
Q04	¿Qué hace crítica esta dependencia y qué cambia si falla, se altera o deja de estar disponible?	Inventario y mapa de dependencias; efecto sobre el servicio; alternativa comprobable	04
Q05	¿Los requisitos de seguridad, datos, cambios, evidencia y terminación necesarios están definidos y acordados?	Contrato y anexos del servicio exacto; requisitos trazados a riesgos; revisión de diferencias	05
Q06	¿Qué diligencia se ha realizado antes de contratar o incorporar el componente?	Identidad y procedencia; documentación; informes con alcance; pruebas de evaluación	06
Q07	¿Qué datos recibe, genera, conserva o reutiliza el proveedor, con qué finalidad y durante cuánto tiempo?	Condiciones de datos y configuración aplicables; regiones, acceso, borrado y uso para entrenamiento; contraste de lo pactado y configurado	07, 05
Q08	¿Qué subproveedores y dependencias relevantes intervienen y cómo se comunican sus cambios?	Lista pertinente, ubicaciones y funciones; condiciones de cambio; revisión del efecto sobre nuestro uso	07
Q09	¿Se pueden limitar y revocar identidades, claves y permisos de la integración?	Configuración de permisos; segregación; ensayo de revocación sin exponer secretos	07

ID	Pregunta	Evidencia y comprobación sugeridas	GV.SC
Q10	Si usamos una API, ¿cómo se limitan solicitudes, destinos, registros y acciones permitidas?	Arquitectura y configuración propia; minimización; pruebas de límites, errores y trazabilidad. No enviar datos sensibles en el ensayo	07
Q11	¿Cómo se conocen, corrigen y comprueban vulnerabilidades del servicio o del componente?	Canal de vulnerabilidades; política de soporte; versiones y comprobación de correcciones pertinentes	09
Q12	Si hay fine-tuning, ¿qué procedencia, permisos, calidad y trazabilidad tienen los datos y resultados del ajuste?	Expediente de datos; autorizaciones; versión y transformación; evaluación de reutilización o exposición	07
Q13	Si hay fine-tuning, ¿cómo se separan entornos y artefactos y cómo se limita el acceso al modelo ajustado?	Configuración de aislamiento; permisos; pruebas de acceso y de exposición pertinentes al riesgo	09
Q14	Si se incorpora un modelo de terceros, ¿conocemos su origen, versión, integridad, condiciones de uso y dependencias?	Publicador y repositorio autorizado; licencia; identificadores de versión; comprobación de integridad y dependencias	06
Q15	¿Qué pruebas propias comprueban calidad, seguridad y supervisión para el uso previsto?	Protocolo y resultados con límites; pruebas de fallo, exposición o manipulación pertinentes; criterios de aceptación separados	09
Q16	¿Cómo se conocen, evalúan y autorizan cambios de modelo, API, datos o condiciones?	Acuerdo de aviso; historial; CAM-001; pruebas de regresión y reversión cuando proceda	09, 05
Q17	¿Cómo colaborará el proveedor en detección, investigación y comunicaciones de incidentes?	Contacto probado; condiciones de aviso y apoyo; datos que entregará; contraste con nuestros plazos de comunicación	08, 05
Q18	¿Qué permite continuar o recuperar el servicio si falla esa dependencia?	Objetivos justificados; restauración o alternativa ensayada; coordinación con proveedor	08

ID	Pregunta	Evidencia y comprobación sugeridas	GV.SC
Q19	¿Cómo se revisan durante la relación el desempeño, las evidencias y los riesgos pendientes?	Revisión por riesgo y por cambios; indicadores; registro de carencias y decisiones	07, 09
Q20	¿Qué ocurre al terminar la relación con datos, accesos, modelos ajustados y continuidad?	Plan de salida; portabilidad pertinente; retirada de permisos; devolución o borrado y forma de comprobarlo	10

Los códigos abreviados de la tabla representan GV.SC-01 a GV.SC-10. Las preguntas Q01-Q04 incluyen trabajo interno de la organización: no se resuelven enviando todas las preguntas al proveedor.

5. Cómo decidir sin esconder las carencias en una puntuación

No se calcula un porcentaje de cumplimiento. Veinte respuestas afirmativas no garantizan que se hayan probado los controles. Una carencia decisiva no queda compensada por muchas respuestas sobre cuestiones menos relevantes.

Antes de evaluar se definen **condiciones de bloqueo para el uso propuesto**. Son decisiones internas basadas en riesgo y requisitos. Como ejemplos:

Condición	Consecuencia de evaluación propuesta
No hay fundamento ni condiciones suficientes para el tratamiento y reutilización de los datos previstos	No autorizar su envío al proveedor hasta resolverlo; reconsiderar datos y modalidad de evaluación
No puede limitarse un acceso con capacidad de actuar sobre un servicio relevante	No autorizar esa capacidad; evaluar una integración con permisos distintos y comprobarla
No existe un modo suficiente de obtener avisos y colaboración para cumplir nuestras obligaciones de incidente	No autorizar la dependencia crítica en ese alcance hasta establecer y probar la coordinación
Un cambio relevante del proveedor no puede conocerse ni comprobarse y hace insuficientes las pruebas existentes	Revisar o detener la autorización del cambio según el procedimiento; no extender automáticamente la evaluación anterior
La salida del proveedor dejaría una dependencia relevante sin tratamiento suficiente	Resolver continuidad y salida o someter una alternativa concreta a decisión de la autoridad competente

El evaluador registra si la conclusión es: **propuesta de autorización para un alcance definido**, **pendiente de resolver carencias** o **propuesta de rechazo**. La autoridad competente decide con evidencia y límites. La ficha de evaluación, por sí sola, no es esa autorización.

Una evaluación con datos sintéticos necesita también alcance, seguridad y autorización interna. No se autoriza automáticamente por excluir datos personales, ni su resultado valida el posterior uso con datos reales.

6. Ficha de decisión

Evaluación: [ID y versión]. Uso: [Completar]. Datos, permisos y entorno: [Completar]. Requisitos examinados: [Completar]. Evidencias suficientes: [Localizadores]. Carencias: [Completar]. Condiciones de bloqueo aplicables: [Completar]. Medidas propuestas: [Completar]. Riesgo residual y fundamento: [Completar]. Propuesta del evaluador: [Completar]. Decisión de la autoridad: [Completar únicamente cuando exista]. Límites, vigencia y revisión: [Completar]. Fuente autorizada del estado: [Completar].

Las carencias tienen responsable, fecha y criterio de cierre. Las condiciones no se consideran resueltas al recibir un correo: se verifica la evidencia pertinente. Los datos de identidad y contacto reales se conservan con el acceso que corresponda.

7. Evidencias y registros que se conectan

PROV-001 mantiene la evaluación de la relación. **R-001 e IMP-001** conservan riesgos e impactos; **FD-001**, datos; **CAM-001**, cambios; **MON-001**, seguimiento; **INC-001**, incidentes y comunicaciones. Se enlazan versiones y localizadores en lugar de mantener copias contradictorias de un mismo estado.

La autoridad de la información se define por dato y alcance. El estado de un proveedor no autoriza todas sus APIs, regiones o modelos. La aceptación de un contrato no autoriza el despliegue de v2 de SYS-003, que sigue **probada, sin autorización de despliegue**.

8. Actividad resuelta: «Tiene certificación, ya podemos conectar»

Enunciado hipotético: un proveedor aporta una certificación vigente sobre parte de sus servicios, pero faltan las condiciones de reutilización de datos y la prueba de revocación de la clave de nuestra integración.

Qué. Conservar la certificación como evidencia acotada y dejar pendiente la autorización de la integración propuesta.

Por qué. No resuelve por sí sola las condiciones del tratamiento ni el control de los accesos propios.

Cómo. Comprobar alcance del certificado; obtener condiciones y configuración aplicables; revisar riesgos y permisos; ensayar revocación; documentar carencias y someter el expediente completo a la autoridad competente.

Cuándo. Antes de enviar los datos o habilitar los permisos del uso propuesto.

Dónde. En PROV-001, con enlaces al expediente de datos, accesos, riesgos y cambio.

Con qué. Contrato, configuración efectiva, evidencia del emisor de la certificación, pruebas propias y personas con autoridad para decidir.

Fuentes

F1. NIST CSF 2.0 y Core oficial con los identificadores de subcategorías. Se utilizan exclusivamente los identificadores vigentes de GV.SC, no elementos retirados de CSF 1.1.

F2. NIST SP 1305: guía de inicio para gestión del riesgo de ciberseguridad en la cadena de suministro. Apoya la organización de la capacidad de evaluación y la definición de requisitos a terceros.

F3. ISO/IEC 42001:2023 y UNE: presentación institucional de las áreas del anexo A. Conexión funcional principal A.10 y complementaria A.7; selección justificada de controles según el SGIA.

F4. Directiva (UE) 2022/2555, artículo 21.2.d y 21.3: seguridad de las relaciones con proveedores directos y consideración de sus vulnerabilidades y prácticas pertinentes.

Detección y cobertura

C3-H06 · José Manuel Hernández Agudo · 25/10/2026

Finalidad

Comprobar que las señales recorren la cadena hasta una función capaz de atenderlas y documentar los puntos ciegos.

Conexión con el SGIA

Seguimiento, MON-001, operación e investigación. Reutiliza registros y localizadores existentes; identifica la fuente autorizada de cada dato y conserva las revisiones.

Campos de la ficha

1. **Escenario y señal:** [Completar con evidencia o pendiente justificado].
2. **Fuente y alcance:** [Completar con evidencia o pendiente justificado].
3. **Regla y criterio interno:** [Completar con evidencia o pendiente justificado].
4. **Responsable y suplente:** [Completar con evidencia o pendiente justificado].
5. **Ensayo y eventos previstos:** [Completar con evidencia o pendiente justificado].
6. **Registros recibidos:** [Completar con evidencia o pendiente justificado].
7. **Alertas generadas:** [Completar con evidencia o pendiente justificado].
8. **Avisos recibidos y triaje:** [Completar con evidencia o pendiente justificado].
9. **Conclusión, límites y acción:** [Completar con evidencia o pendiente justificado].

Cómo trabajarla

Primero delimita el alcance y distingue hechos, propuestas y datos pendientes. Consulta las fuentes y registros pertinentes. Completa la ficha sin copiar secretos ni datos personales innecesarios. Vincula la evidencia que sostiene cada conclusión y asigna responsable y siguiente paso a las carencias. Una propuesta no se registra como actuación realizada ni como decisión autorizada.

Modelo del ejercicio

Los datos siguientes son didácticos; los supuestos adicionales no acreditan implantación ni incidentes reales en la empresa ficticia.

Campo	Respuesta orientativa
Escenario y señal	C3-DET-01, diez eventos sintéticos que debían detectarse
Fuente y alcance	Fuente de ensayo y colector definidos en el supuesto
Regla y criterio interno	Observar por separado recepción, alerta y entrega; criterio interno del ejercicio
Responsable y suplente	Función de guardia de ejercicio; confirmar titulares al aplicar
Ensayo y eventos previstos	Diez eventos identificados; etapas anidadas
Registros recibidos	9 de 10: 90 %

Campo	Respuesta orientativa
Alertas generadas	8 de 10: 80 %; 8 de los 9 recibidos si se declara ese denominador
Avisos recibidos y triaje	7 de 10: 70 %; triaje posterior no cuantificado en el supuesto
Conclusión, límites y acción	No demuestra cobertura global ni tasa de falsas alarmas; investigar pérdidas y repetir prueba pertinente

Antes de cerrar

Un caso sin hito final no tiene latencia cero. La ausencia de registro se distingue de ausencia del evento.

La persona revisora debe poder reconstruir alcance, evidencia, límites, responsable y decisión. Se mantienen las autorizaciones del caso; v2 de SYS-003 sigue probada, sin autorización de despliegue.

Formularios de clasificación y comunicaciones

Complemento de C3-H07 · Extensión de INC-001 · José Manuel Hernández Agudo · 25/10/2026

Se copian en el expediente del incidente. Los campos sin evidencia se identifican como pendientes; no se cumplimentan con datos inventados. Los modelos ayudan a preparar la información: cuando exista un formulario oficial aplicable, se utiliza y se conserva su versión. Estos documentos no envían comunicaciones.

F01. Ficha de análisis y decisión

- Identificador del incidente en INC-001: [Completar].
- Entidad y servicio: [Completar].
- Sistemas, usos, versiones y entornos conocidos: [Completar].
- Hechos y fuentes: [Completar; localizar evidencia protegida].
- Hipótesis y preguntas pendientes: [Completar].
- T_detección, zona horaria y fuente: [Completar].
- Régimen aplicable a entidad y servicio: [Norma, versión, artículo y justificación].
- Criterios de significatividad examinados: [Criterio / evidencia / conclusión / pendiente].
- Criterios suficientes identificados, si existen: [Completar].
- Conclusión: [Significativo / no se acredita significatividad con lo examinado / evaluación pendiente; justificar alcance].
- T_constancia, zona horaria y fundamento: [Completar; conservar revisiones].
- Responsable de la evaluación y de la siguiente comprobación: [Completar].
- Medidas y escalado inmediato: [Completar].
- Destinatario y canal oficial verificado: [Completar].
- Remitente autorizado y suplente: [Completar].
- Ventana general o excepción aplicable: [Completar].
- Máximo de alerta temprana: [T_constancia + 24 horas; verificar régimen].
- Máximo de notificación: [T_constancia + 72 horas en régimen general; comprobar excepción de confianza].
- Momento real de notificación de la letra b: [Completar con justificante].
- Fecha máxima del informe final: [Un mes desde esa notificación; confirmar cómputo].
- Próxima revisión: [Responsable, hito y fecha].

F02. Información para la alerta temprana

Tipo: alerta temprana. Referencia interna: [Completar]. Entidad y contacto autorizado: [Completar]. Destinatario y canal: [Completar]. Fecha, hora y zona: [Completar].

Servicio afectado: [Completar]. Hechos disponibles y situación: [Completar]. Momento de constancia del incidente significativo y criterio utilizado: [Completar]. Sospecha de actuación ilícita o malintencionada, cuando proceda: [Indicar hechos que la sustentan; no equiparar causa desconocida con ataque]. Posibles repercusiones transfronterizas: [Completar o indicar lo que se está comprobando]. Medidas iniciales: [Completar]. Información pendiente y siguiente actualización: [Completar].

Control de remisión: versión exacta enviada [Localizador]; remitente [Completar]; fecha y hora reales [Completar]; justificante y referencia oficial [Localizador]; incidencias del canal [Completar].

F03. Información para la notificación del incidente

Tipo: notificación de la letra b. Referencia oficial e interna: [Completar]. Actualización de la alerta: [Completar]. Evaluación inicial de gravedad e impacto: [Completar]. Servicios, entidades o personas afectadas o potencialmente afectadas: [Completar con alcance y limitaciones]. Indicadores de compromiso disponibles: [Completar o indicar que no se dispone de indicadores verificados]. Medidas aplicadas y en curso: [Completar]. Hipótesis de causa y grado de soporte: [Completar]. Repercusiones transfronterizas conocidas o posibles: [Completar]. Pendientes, responsables y próxima actualización: [Completar].

Control de remisión: versión, remitente, T_envío, justificante y referencia oficial [Completar]. Máximo del informe final calculado desde este envío [Completar].

F04. Informe intermedio, de situación o final

Tipo y motivo: [Solicitud de autoridad / informe de situación por incidente en curso / informe final]. Referencia y fecha: [Completar]. Descripción y cronología: [Completar]. Gravedad e impacto con evidencia: [Completar]. Amenaza o causa principal probable y fundamento: [Completar; separar certeza e hipótesis]. Medidas aplicadas y en curso: [Completar]. Repercusiones transfronterizas, cuando proceda: [Completar]. Situación de recuperación y evidencia de comprobación: [Completar]. Pendientes y seguimiento: [Completar]. Hito de gestión del incidente, si procede: [Completar y justificar]. Remisión y justificante: [Completar].

Un informe final no requiere inventar una causa demostrada. Debe expresar la conclusión disponible y el soporte de la causa probable, así como las medidas y los pendientes que correspondan.

F05. Otras rutas de comunicación

NIS2 / disposición aplicable

Sujeto y rol: [Completar] · **Hecho que activa la ruta:** [Completar] · **Momento de conocimiento propio:** [Completar] · **Destinatario y canal:** [Completar] · **Plazo y fuente:** [Completar] · **Responsable y justificante:** [Completar]

Protección de datos

Sujeto y rol: [Responsable o encargado; consultar al DPD cuando corresponda] · **Hecho que activa la ruta:** [Completar] · **Momento de conocimiento propio:** [Completar] · **Destinatario y canal:** [Completar] · **Plazo y fuente:** [Completar] · **Responsable y justificante:** [Completar]

AI Act, si corresponde

Sujeto y rol: [Rol, sistema y disposición aplicable] · **Hecho que activa la ruta:** [Completar] · **Momento de conocimiento propio:** [Completar] · **Destinatario y canal:** [Completar] · **Plazo y fuente:** [Completar] · **Responsable y justificante:** [Completar]

Destinatarios del servicio

Sujeto y rol: [Completar] · **Hecho que activa la ruta:** [Completar] · **Momento de conocimiento propio:** [Completar] · **Destinatario y canal:** [Completar] · **Plazo y fuente:** [Completar] · **Responsable y justificante:** [Completar]

Contrato con cliente o proveedor

Sujeto y rol: [Completar] · **Hecho que activa la ruta:** [Completar] · **Momento de conocimiento propio:** [Completar] · **Destinatario y canal:** [Completar] · **Plazo y fuente:** [Completar] · **Responsable y justificante:** [Completar]

Cada ruta conserva su fundamento, reloj y evidencia de envío. No se copia automáticamente el momento NIS2 al resto. La prueba docente se realiza sin remitir formularios a autoridades, clientes o proveedores reales.

Evaluar y notificar un incidente significativo

C3-H07 · Procedimiento y extensión de INC-001 · Herramienta para la lección 7

José Manuel Hernández Agudo · Monográfico 3 · 25/10/2026

1. Objeto y preparación

Este procedimiento organiza la evaluación de un incidente, los plazos de comunicación y su trazabilidad en el SGIA. Se adapta al servicio y a la entidad antes de aprobarlo para uso operativo. La autoridad, los canales y la normativa aplicable deben estar identificados; el ejercicio no presupone que Tech Server IIT Spain esté comprendida en una categoría jurídica concreta.

Antes de una emergencia deben constar: responsable y suplente de incidentes; remitente autorizado; contacto de asesoría y del DPD cuando corresponda; autoridad o CSIRT competente y canal oficial; credenciales y acceso alternativo al canal; servicios y proveedores incluidos; reglas de clasificación; contratos y obligaciones paralelas. Se comprueba que el suplente puede actuar. Los datos de contacto se mantienen en un registro protegido y actualizado, no en la edición pública del curso.

La base europea de las ventanas estudiadas es el artículo 23 de NIS2. Se identifica además el régimen nacional y sectorial pertinente. El Reglamento de Ejecución (UE) 2024/2690 detalla criterios para las entidades que comprende su artículo 1. Utilizar una API de IA no demuestra por sí solo pertenecer a una de ellas. [F1, F2]

2. De una señal a una obligación

Se distinguen tres preguntas:

1. **¿Qué sucedió?** Registrar hechos, datos afectados, servicio, versión y entorno; diferenciar señal, sospecha y compromiso observado.

2. **¿Es un incidente y es significativo en el régimen aplicable?** Analizar compromiso de disponibilidad, autenticidad, integridad o confidencialidad de datos o servicios y sus consecuencias reales o posibles.

3. **¿Quién debe comunicar qué, a quién y cuándo?** Identificar entidad obligada, destinatarios, momento de constancia y contenido exigido.

Un fallo algorítmico no se convierte automáticamente en incidente significativo por superar un porcentaje interno. Tampoco se descarta por no existir un ataque: una causa accidental puede comprometer un servicio. Una fuga de datos puede abrir varias rutas simultáneas, cada una con destinatario, criterio y reloj propios.

Criterio general del artículo 23.3

La Directiva contempla las graves perturbaciones operativas de los servicios o pérdidas económicas que el incidente haya causado o pueda causar a la entidad, y los perjuicios materiales o inmateriales considerables que haya causado o pueda causar a otras personas físicas o jurídicas. La evaluación debe atender a esos supuestos y a sus concreciones aplicables. No se exige esperar a que el perjuicio potencial se materialice. [F1]

No existe en ese artículo un porcentaje universal de errores de IA, un número universal de registros filtrados ni una cuantía única para todas las entidades. En cada expediente se identifica el criterio jurídico utilizado y la evidencia que lo satisface, lo descarta o aún falta.

3. Criterios concretos del Reglamento 2024/2690

Esta sección se utiliza cuando la entidad y el servicio pertenecen al ámbito de ese Reglamento. No sustituye las reglas de otros sectores. Los artículos 3 y 4 se revisan junto con el artículo específico del servicio: comprobar solo un umbral financiero puede omitir otra causa de significatividad. [F2]

Artículos 3 y 4: condiciones comunes

Referencia	Condición que se examina
Art. 3.1.a	Pérdidas financieras directas causadas o posibles superiores a 500.000 euros o al 5 % del volumen de negocios total anual del ejercicio anterior, tomando el importe menor.
Art. 3.1.b	Exfiltración causada o posible de secretos comerciales de la entidad, en el sentido legal indicado por el Reglamento.
Art. 3.1.c-d	Muerte o daños considerables a la salud de una persona física, causados o posibles.
Art. 3.1.e	Acceso efectivamente producido, presuntamente malicioso y no autorizado, que pueda causar graves perturbaciones operativas.
Art. 3.1.f y art. 4	Al menos dos incidentes en seis meses, misma causa fundamental aparente y cumplimiento colectivo del criterio financiero del art. 3.1.a. Deben concurrir las tres condiciones.
Art. 3.1.g	Cumplimiento de uno o más criterios del artículo específico pertinente, entre los artículos 5 y 14.

El límite financiero se expresa como **L = mínimo de 500.000 euros y 0,05 × volumen de negocios total anual del ejercicio anterior**. La condición usa **superior a L**; no equivale a «igual o superior». No cumplir este criterio no descarta los demás.

Las interrupciones programadas y las consecuencias previstas del mantenimiento programado tienen el tratamiento del artículo 3.2. Esa previsión no permite etiquetar como mantenimiento cualquier compromiso inesperado de seguridad. Al contar usuarios se sigue el artículo 3.3: el cómputo no se reduce necesariamente al número de contratos o de tickets.

Ejemplo sectorial completo: servicios gestionados y de seguridad gestionados, artículo 10

Se aplica únicamente tras justificar que la actividad examinada pertenece a esa categoría.

Supuesto del artículo 10	Condición
a. Indisponibilidad completa	El servicio está completamente indisponible durante **más de 30 minutos**.
b. Disponibilidad limitada	Afecta a **más del 5 % de los usuarios del servicio en la Unión o a más de un millón, tomando el número menor**, durante **más de una hora**.
c. Compromiso por acción presuntamente malintencionada	Se compromete la integridad, confidencialidad o autenticidad de datos relacionados con la prestación, como consecuencia de una acción presuntamente malintencionada. No añade en esta letra un mínimo de usuarios ni de duración.
d. Compromiso con alcance de usuarios	Se compromete la integridad, confidencialidad o autenticidad de esos datos y afecta a **más del 5 % de los usuarios del servicio en la Unión o a más de un millón, tomando el número menor**. Esta letra no añade una duración mínima.

Para b y d: **U = mínimo de 0,05 × usuarios del servicio en la Unión y 1.000.000**. Debe superarse U; en b también debe superarse una hora. El denominador pertenece al servicio y al ámbito geográfico indicado, no a una muestra de validación de un modelo.

Ejemplo de cálculo: con 2.000 usuarios del servicio en la Unión, U = 100. Si se han contabilizado correctamente 101 afectados, se supera el criterio de usuarios; con 100 no. Para b aún se comprueba la

duración. Incluso si no se supera U, se revisan a, c y los criterios comunes que procedan.

La caída de 9/10 a 7/10 críticos detectados por SYS-003 no es este porcentaje de usuarios y no se compara con ese 5 %. El criterio didáctico de rendimiento del curso y el umbral jurídico describen magnitudes distintas.

4. Activación y relojes

OPS registra la señal y avisa al responsable de incidentes. CISO coordina la evaluación técnica; AIO aporta contexto de finalidad, versión, supervisión e impactos de IA; asesoría ayuda a determinar aplicabilidad, destinatario y obligación. Se ejecutan protección y preservación de evidencia mientras se evalúa la comunicación.

Se registran como mínimo:

- **T_detección:** primera señal conocida, con fuente y hora.
- **T_constancia:** momento en que la entidad tiene constancia del incidente significativo, con hechos y razonamiento.
- **T_envío:** momento real de cada comunicación, con justificante.
- **T_gestionado:** hito relevante para el informe final cuando el incidente continúe en curso; debe justificarse.

T_constancia no se elige esperando una firma, una reunión o la causa raíz definitiva. El registro debe reflejar cuándo se tuvo efectivamente constancia. Si la reconstrucción posterior muestra que ocurrió antes, se corrige de forma trazable, sin borrar la anotación anterior, y se reevalúan los plazos.

Cuando la significatividad siga pendiente se escala con urgencia, se asigna una comprobación y se preparan comunicaciones con los hechos disponibles. No se usa «en evaluación» para suspender indefinidamente la actuación. Como control interno prudente pueden calcularse ventanas provisionales desde el momento más temprano razonablemente posible; no reemplazan el análisis del momento legal de constancia.

Tabla de comunicaciones del artículo 23.4

Comunicación	Referencia temporal	Contenido principal
Alerta temprana	Sin demora indebida y como máximo **24 horas desde T_constancia**	Señalar, cuando proceda, sospecha de actuación ilícita o malintencionada y posibles repercusiones transfronterizas. Identificar incidente, entidad, servicio y contacto para el seguimiento.
Notificación del incidente	Sin demora indebida y como máximo **72 horas desde el mismo T_constancia**	Actualizar lo anterior y aportar evaluación inicial de gravedad e impacto e indicadores de compromiso cuando estén disponibles.
Informe intermedio	Cuando lo solicite el CSIRT o la autoridad competente	Actualizaciones pertinentes sobre la situación conforme a la solicitud.
Informe final	Como máximo **un mes después de presentar la notificación de la letra b**	Descripción, gravedad e impacto, amenaza o causa probable, medidas aplicadas y en curso y repercusiones transfronterizas cuando proceda.
Incidente que sigue en curso en ese hito	Informe de situación en ese momento; informe final dentro de **un mes desde que se haya gestionado el incidente**	Situación, actuaciones y evolución; completar posteriormente el informe final.

Excepción de servicios de confianza: para los incidentes significativos que afecten a la prestación de esos servicios, la notificación de la letra b se realiza sin demora indebida y, en todo caso, dentro de **24 horas desde la constancia**. No se aplica automáticamente la ventana general de 72 horas. [F1]

Las 72 horas no comienzan después de la alerta temprana. Las ventanas expresadas en horas no se convierten en días laborables. El mes no se sustituye por 30 días; el cómputo de fechas y sus reglas aplicables se confirma en el expediente. Los límites son máximos: no autorizan una espera innecesaria.

El informe inicial identifica lo conocido, las hipótesis, lo pendiente y la siguiente actualización. No se inventan indicadores de compromiso. Una hipótesis de exfiltración no se comunica como fuga confirmada. Se conserva la versión exacta enviada y cualquier corrección posterior.

5. Secuencia de ejecución

1. **Registrar y proteger.** Abrir un identificador de incidente; preservar las fuentes pertinentes y aplicar las medidas de contención autorizadas. Evitar que la captura de evidencia agrave el daño.

2. **Precisar el alcance.** Confirmar entidad, servicio, entorno, versiones efectivas, usuarios y proveedores; documentar incertidumbres.

3. **Evaluar la significatividad.** Aplicar las reglas pertinentes, incluidas las consecuencias potenciales; registrar cada criterio y su evidencia. Si hay un criterio suficiente, no esperar a cerrar todos los restantes para actuar.

4. **Determinar la comunicación.** Confirmar destinatario, canal y remitente; calcular relojes y suplencias. La falta del titular no bloquea el procedimiento aprobado.

5. **Enviar y conservar.** Remitir la comunicación exigible sin demora indebida y dentro del máximo; conservar justificante, referencia oficial y copia controlada. Si falla el canal, usar la alternativa oficial prevista y dejar constancia de intentos y escalado.

6. **Actualizar e investigar.** Atender solicitudes; revisar impactos, proveedores e hipótesis; mantener las comunicaciones que correspondan sin esperar una investigación perfecta.

7. **Recuperar y comprobar.** Verificar el servicio y la integridad de lo recuperado; conservar evidencia de la decisión de continuidad o vuelta al servicio.

8. **Cerrar y mejorar.** Completar informes y medidas; comprobar eficacia; trasladar lecciones a riesgos, proveedores, cambios y formación. Servicio restablecido y expediente cerrado pueden ser estados diferentes.

La remisión al CSIRT o a la autoridad no cubre automáticamente las comunicaciones a destinatarios de servicios previstas en los artículos 23.1 y 23.2. Se evalúan separadamente, al igual que las obligaciones de protección de datos, AI Act y contratos. Avisar a un proveedor o cliente tampoco sustituye por sí solo una notificación oficial.

6. Integración con INC-001 y el SGIA

INC-001 es el registro del curso; dentro de él cada incidente conserva su identificador. La herramienta añade campos de clasificación y comunicaciones al expediente existente. No crea otro registro con un estado contradictorio.

Parte del trabajo	Conexión funcional	Evidencia que conservar
Preparación, autoridad y suplencias	Gobierno del SGIA; organización interna	Procedimiento aprobado, roles y prueba del canal
Detección e investigación	MON-001 e INC-001; operación y seguimiento	Señales, cronología, versiones y hechos

Parte del trabajo	Conexión funcional	Evidencia que conservar
Datos y exposición	Área A.7: datos para sistemas de IA	Datos afectados, acceso, trazabilidad y medidas
Comunicaciones	Área A.8: información para partes interesadas	Destinatarios, mensajes, plazos y justificantes
Restricción o continuidad del uso	Área A.9: uso de sistemas de IA	Decisiones sobre uso, supervisión y límites
Coordinación con terceros	Área A.10: relaciones con terceros y clientes	Acuerdos, avisos y reparto de actuaciones
Corrección y eficacia	Riesgos, impactos, cambios y mejora	R-001, IMP-001, CAM-001 y comprobaciones vinculadas

La comunicación de incidentes no debe atribuirse únicamente a A.9. Este mapa se formula por áreas funcionales, sin reproducir cláusulas ni declarar equivalencia normativa completa. La selección de controles del SGIA se justifica según su contexto y tratamiento de riesgos. [F3]

INC-001 conservará: clasificación y revisiones; fundamento y fuentes; T_detección y T_constancia; régimen y destinatarios; máximos calculados; responsable y suplente; mensajes y justificantes; información pendiente; próxima actualización; medidas, recuperación y cierre. La información sensible se guarda con permisos adecuados y se enlaza desde el expediente. La fuente autorizada del estado se identifica por dato; no gana automáticamente la copia más reciente.

7. Comprobación antes de aprobar el procedimiento

Debe poder demostrarse en un ejercicio que el suplente accede al canal, que ambos plazos parten de T_constancia, que la excepción de servicios de confianza se reconoce y que el informe final se calcula desde la notificación de la letra b. Se ensaya también un criterio no financiero y un caso con significatividad pendiente.

Los formularios y el supuesto C3-NOT-01 de esta entrega permiten hacer ese ejercicio sin enviar comunicaciones reales.

Fuentes

F1. Directiva (UE) 2022/2555: artículos 6, 20, 21 y 23.

F2. Reglamento de Ejecución (UE) 2024/2690: artículos 1, 3, 4 y 10.

F3. UNE: presentación institucional sobre ISO/IEC 42001, áreas del anexo A y ficha oficial ISO/IEC 42001:2023.

F4. NIST CSF 2.0: relación funcional con detectar, responder, comunicar y recuperar. Esta herramienta es una elaboración docente del curso.

Recuperación y eficacia

C3-H08 · José Manuel Hernández Agudo · 25/10/2026

Finalidad

Comparar resultados de recuperación con objetivos previos y comprobar si las mejoras resuelven la carencia que las motivó.

Conexión con el SGIA

Continuidad, cambios, evaluación y mejora del SGIA. Reutiliza registros y localizadores existentes; identifica la fuente autorizada de cada dato y conserva las revisiones.

Campos de la ficha

1. **Servicio y supuesto:** [Completar con evidencia o pendiente justificado].
2. **Objetivos previos y fundamento:** [Completar con evidencia o pendiente justificado].
3. **Inicio y condiciones de medición:** [Completar con evidencia o pendiente justificado].
4. **Restauración técnica:** [Completar con evidencia o pendiente justificado].
5. **Recuperación con comprobaciones:** [Completar con evidencia o pendiente justificado].
6. **Punto de datos recuperado:** [Completar con evidencia o pendiente justificado].
7. **Resultados por criterio:** [Completar con evidencia o pendiente justificado].
8. **Decisión y límites:** [Completar con evidencia o pendiente justificado].
9. **Acción, evidencia y nueva comprobación:** [Completar con evidencia o pendiente justificado].

Cómo trabajarla

Primero delimita el alcance y distingue hechos, propuestas y datos pendientes. Consulta las fuentes y registros pertinentes. Completa la ficha sin copiar secretos ni datos personales innecesarios. Vincula la evidencia que sostiene cada conclusión y asigna responsable y siguiente paso a las carencias. Una propuesta no se registra como actuación realizada ni como decisión autorizada.

Modelo del ejercicio

Los datos siguientes son didácticos; los supuestos adicionales no acreditan implantación ni incidentes reales en la empresa ficticia.

Campo	Respuesta orientativa
Servicio y supuesto	Servicio adicional C3-REC-01, separado de SYS-003 y T10-014
Objetivos previos y fundamento	RTO 2 horas y RPO 15 minutos; criterios internos del supuesto
Inicio y condiciones de medición	09:00; se incluyen verificaciones funcionales y de seguridad
Restauración técnica	10:35, 95 minutos
Recuperación con comprobaciones	10:50, 110 minutos
Punto de datos recuperado	08:40: antigüedad de 20 minutos respecto de las 09:00

Campo	Respuesta orientativa
Resultados por criterio	Tiempo cumple; punto de datos no cumple el objetivo de 15 minutos
Decisión y límites	No declarar satisfacción completa; elevar carencia y alternativas
Acción, evidencia y nueva comprobación	Comprobar otras fuentes y mejorar recuperación; repetir ensayo y verificar eficacia sin inventar datos perdidos

Antes de cerrar

Servicio restablecido, incidente cerrado y mejora eficaz son conclusiones distintas que requieren soporte pertinente.

La persona revisora debe poder reconstruir alcance, evidencia, límites, responsable y decisión. Se mantienen las autorizaciones del caso; v2 de SYS-003 sigue probada, sin autorización de despliegue.

H01. Alcance y aplicabilidad

Completa con hechos, evidencias, límites y decisiones identificadas.

Alcance y versiones

Fuentes y fundamento

Conclusión y límites

Autoridad y suplencias

Pendientes y siguiente paso

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H02. Perfil y prioridades

Completa con hechos, evidencias, límites y decisiones identificadas.

Resultado actual y soporte

Objetivo y brecha

Prioridad razonada

Actuación, autoridad y medios

Comprobación del cierre

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H03. Activos, dependencias y escenarios

Completa con hechos, evidencias, límites y decisiones identificadas.

Cadena del servicio y límites

Activos y responsabilidades

Escenarios y consecuencias

Fuentes y evidencia

Comprobaciones pendientes

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H04. Protección y pruebas

Completa con hechos, evidencias, límites y decisiones identificadas.

Riesgo y medida

Criterio previo

Ensayo y condiciones

Resultado y límites

Decisión y evidencia

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H05. Proveedor y cambio

Completa con hechos, evidencias, límites y decisiones identificadas.

Servicio, finalidad y datos

Evidencias y alcance

Carencias decisivas

Propuesta y autoridad

Seguimiento y cierre

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H06. Detección y cobertura

Completa con hechos, evidencias, límites y decisiones identificadas.

Escenario, fuente y señal

Regla y responsabilidad

Ensayo por etapas

Resultados y denominadores

Puntos ciegos y acciones

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H07. Incidente y comunicaciones

Completa con hechos, evidencias, límites y decisiones identificadas.

Hechos, hipótesis y alcance

Criterio y fundamento jurídico

Detección y constancia

Destinatarios, máximos y envíos

Medidas, pendientes y revisión

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

H08. Recuperación y eficacia

Completa con hechos, evidencias, límites y decisiones identificadas.

Objetivos y criterio

Ensayo y alcance

Resultados de tiempo y datos

Decisión y limitaciones

Mejora y prueba de eficacia

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Tres ejemplos para trabajar gobierno, notificación y proveedores

José Manuel Hernández Agudo · Monográfico 3 · 25/10/2026

Tech Server IIT Spain es una empresa ficticia. Los supuestos adicionales se identifican expresamente. Los documentos, contactos, fechas de incidentes y respuestas de proveedores que se crean para estos ejemplos son **datos simulados**, no actuaciones realizadas ni evidencias reales de terceros.

1. RACI de la lección 1: expediente de evaluación de SYS-003

Identificador: C3-H01A-EJ-01, versión didáctica 1. **Entidad:** Tech Server IIT Spain. **Alcance:** SYS-003 / USO-004 / v2, entorno de evaluación del supuesto C3-ALC-01. **Estado que se conserva:** probada, sin autorización de despliegue. **Aplicabilidad NIS2:** pendiente del análisis documentado de actividad, tamaño, jurisdicción y disposiciones pertinentes. La preparación de responsabilidades puede comenzar mientras se resuelve.

Órgano de dirección y titulares: no están definidos en el caso canónico; la matriz propone funciones que deben confirmarse, sin atribuir nombramientos a personas concretas. **Fuente del estado:** expediente autorizado del sistema y del cambio que se identifique al completar la ficha; no se inventa su localizador. **Aprobación del modelo:** propuesta docente pendiente de decisión de la organización.

Para este alcance se aplica la matriz de dieciséis tareas de C3-H01A, disponible también en CSV. Tres actuaciones permiten entenderla:

Actuación propuesta	Quien realiza	Quien decide internamente	Evidencia de cierre requerida
Revisar las dos cuentas administrativas del supuesto	OPS, con coordinación de CISO	CISO para el triaje y DG para decisiones fuera de los límites delegados	Inventario, necesidad, permisos, dependencias y prueba de la medida decidida
Confirmar que el trabajo sigue en evaluación	AIO y OPS	DG para las decisiones de autorización que tenga delegadas	Fuente autorizada del estado y límites del entorno
Revisar una desviación relevante de medidas aprobadas	DG, AIO y CISO preparan información	OD supervisa y decide lo que corresponda	Información examinada, decisión, recursos y seguimiento

Plan de formación propuesto: dos horas de gobierno de ciberseguridad, dos de gobierno de IA y una de ejercicio de incidente. **Estado:** plan propuesto; asistencia y resultados no acreditados. **Criterio interno de comprobación:** cada participante debe distinguir un criterio legal de uno interno, interpretar el caso de rendimiento y reconstruir el reloj de comunicaciones del ejercicio. Si no lo demuestra, se documenta apoyo adicional y una nueva comprobación; no se inventa una formación completada.

El ejercicio de rendimiento conserva v1 90/100 global y 9/10 críticos; v2 94/100 y 7/10 críticos. La mejora global es de cuatro puntos porcentuales y la caída en críticos de veinte. Estos resultados no prueban un ciberataque ni autorizan v1 o v2. Los errores globales y críticos pueden solaparse: no se suman como nueve casos distintos.

2. C3-NOT-01: indisponibilidad de un servicio gestionado

Premisas expresas del ejercicio

Se crea un servicio adicional **SVC-C3-01**, separado de SYS-003 y de T10-014. A efectos de este ejercicio, la ficha jurídica ha establecido que a la entidad y al servicio les corresponde el régimen de notificación del artículo 23 NIS2 y el artículo 10 del Reglamento 2024/2690, como proveedor de servicios gestionados. No es un servicio de confianza. Estas premisas no resuelven la aplicabilidad real de NIS2 al caso canónico.

El servicio completo deja de estar disponible por una incidencia no programada. No se acredita aún causa maliciosa ni fuga de datos. Todas las horas del ejemplo son **UTC**, con sufijo Z. Los envíos son simulados a un canal de ejercicio, sin comunicaciones externas.

F01 cumplimentada

Campo	Respuesta del ejercicio
Registro e identificador	INC-001 → C3-NOT-01
Entidad y servicio	Tech Server IIT Spain / SVC-C3-01
Entorno	Operación del servicio adicional definido en este supuesto; no se asigna versión de SYS-003
Primera señal conocida	03/11/2026, 09:10 Z; monitor simulado EV-NOT-01
Hechos comprobados en evaluación inicial	A las 09:30 Z se contrasta indisponibilidad completa desde las 08:55 Z, todavía en curso; evidencias simuladas EV-NOT-01 y EV-NOT-02
Criterio suficiente	Art. 10.a del Reglamento 2024/2690: servicio completo indisponible más de 30 minutos; a las 09:30 han transcurrido 35 minutos
Conclusión del supuesto	Incidente significativo bajo las premisas jurídicas expresas del ejercicio
T_constancia	03/11/2026, 09:30 Z; en este supuesto es el primer momento en que la entidad dispone de los hechos contrastados indicados
Responsable técnico	Función CISO de ejercicio; OPS aporta medidas y registros
Contexto IA	AIO comprueba dependencias y efectos del uso si resultan pertinentes; no atribuye el incidente a SYS-003
Remitente y suplente	DG de ejercicio autoriza conforme al procedimiento; CISO remite; suplente designado para el canal simulado
Destinatario	Autoridad/CSIRT del ejercicio, identificador didáctico DEST-C3-01
Canal	CANAL-NIS2-EJERCICIO, sin dirección ni destinatario real
Máximo de alerta	04/11/2026, 09:30 Z
Máximo de notificación de la letra b	06/11/2026, 09:30 Z
Alerta enviada en simulación	03/11/2026, 10:00 Z; justificante simulado JUS-C3-01
Recuperación observada	03/11/2026, 10:10 Z; prueba de servicio EV-NOT-03; duración total de indisponibilidad: 75 minutos
Notificación de la letra b enviada en simulación	03/11/2026, 14:00 Z; justificante simulado JUS-C3-02
Agenda interna para informe final	03/12/2026, 14:00 Z; planificación conservadora desde la notificación presentada. Confirmar cómputo mensual y calendario; esta hora no es un límite legal universal
Causa y otras rutas	Causa en investigación; sin fuga ni ataque acreditados. Se revisan por separado los hechos y requisitos de otras comunicaciones

Si apareciese evidencia de una constancia anterior, se corregiría de forma trazable el reloj. Los hitos de esta simulación no sirven para elegir una fecha de conocimiento más conveniente.

F02: texto de alerta del ejercicio

Simulación. Referencia C3-NOT-01. Tech Server IIT Spain informa de la indisponibilidad completa no programada de SVC-C3-01, observada en registros desde las 08:55 Z del 03/11/2026 y contrastada a las 09:30 Z. El servicio continúa indisponible al preparar esta alerta. Bajo las premisas del ejercicio, se cumple el artículo 10.a del Reglamento 2024/2690. Se han activado respuesta y preservación de registros. La causa sigue en investigación; no hay datos que acrediten una acción malintencionada ni una fuga. Se está comprobando el alcance geográfico y cualquier repercusión transfronteriza. El contacto operativo es la función CISO del canal simulado; se aportará una evaluación inicial actualizada en la notificación correspondiente.

F03: actualización del ejercicio

Simulación. Referencia C3-NOT-01 / JUS-C3-01. El servicio fue restablecido a las 10:10 Z, con comprobación EV-NOT-03. La indisponibilidad completa duró 75 minutos. La investigación mantiene pendiente el alcance detallado de consecuencias y la causa probable. No se dispone de indicadores de compromiso verificados; ello no demuestra ausencia de ataque. Se conservan registros de configuración y operación para su análisis. La recuperación observada no cierra todavía la investigación ni las acciones. Se mantienen seguimiento y revisión de comunicaciones pertinentes. Notificación de la letra b preparada y remitida en el ejercicio a las 14:00 Z del 03/11/2026.

Prueba de aprendizaje: las 72 horas vencen el 06/11 a las 09:30 Z, aunque la alerta se enviara a las 10:00 Z del día 3. El informe final se calcula desde la notificación de la letra b del día 3 a las 14:00 Z. No se espera a esos máximos si la información puede comunicarse antes sin demora indebida.

Actividad resuelta: esperar a la causa raíz

Enunciado: se propone posponer la alerta hasta confirmar si hubo ataque y hasta la siguiente reunión del consejo.

Qué. Preparar y remitir la comunicación exigible con los hechos disponibles, según la autoridad delegada del procedimiento.

Por qué. El criterio suficiente del supuesto ya se cumple; la causa definitiva y la reunión no reinician ni suspenden el reloj.

Cómo. Conservar T_constancia y el fundamento, activar remitente o suplente, explicar lo pendiente y registrar envío y justificante.

Cuándo. Sin demora indebida y dentro de la ventana aplicable.

Dónde. En INC-001 y en el canal oficial que corresponda en un caso real; este ejercicio usa únicamente un canal simulado.

Con qué. Cronología, evidencia preservada, ficha de aplicabilidad, formulario pertinente y accesos previamente preparados.

3. C3-SUP-01: propuesta de una API de IA de terceros

Se introduce una integración adicional de asistencia denominada **C3-SUP-01**, sin atribuirla a SYS-003. **Proveedor Delta** es un nombre ficticio. El supuesto propone usar una API remota con documentación de soporte interna. No incluye fine-tuning ni descarga de un modelo. Las respuestas y los documentos EV-SUP son datos de ejercicio; no se aportan como informes auténticos.

Las veinte respuestas cumplimentadas figuran también en C3-H05_Ejemplo_C3_SUP01.csv. El modelo no deja ninguna pregunta sin conclusión: dos se justifican como no aplicables y las restantes describen el alcance de la evidencia o la carencia.

Cuestión decisiva	Respuesta de ejercicio	Conclusión y acción
Q07. Uso de datos	La condición contractual simulada no aclara si el contenido enviado puede	No evidenciado para el uso propuesto. Bloquear envío de datos internos

Cuestión decisiva	Respuesta de ejercicio	Conclusión y acción
	reutilizarse para mejorar modelos ni su retención completa	reales hasta acordar condiciones y comprobar configuración
Q09. Revocación	La clave de ensayo puede revocarse y deja de permitir llamadas según prueba simulada EV-SUP-03	Suficiente para esa prueba; revisar permisos y alcance del entorno definitivo
Q12-Q13. Fine-tuning	No se contrata ni se realiza en el alcance definido	No aplica, con justificación; si se introduce, reabrir evaluación
Q17. Incidentes	Existe una dirección genérica de soporte; no se ha probado la vía de emergencia ni el compromiso de información necesario	Parcial. Resolver y ensayar coordinación antes de autorizar la dependencia en el alcance propuesto
Q20. Salida	Hay exportación de registros propios, pero no evidencia suficiente sobre el borrado del contenido conservado por el proveedor	Parcial. Definir alcance de salida y obtener evidencia pertinente

Propuesta del evaluador: pendiente de resolver carencias; no autorizar todavía el uso con documentación interna real. Una evaluación limitada con datos sintéticos podría proponerse como alternativa, pero requeriría su propia autorización y no demostraría la adecuación posterior del uso real.

Decisión de la autoridad: no emitida en el supuesto. **Seguimiento:** Compras y asesoría proponen aclaraciones contractuales; CISO prepara pruebas de coordinación y configuración; AIO revisa finalidad y riesgos; OPS documenta la alternativa. Se identifican responsables nominales, fechas y localizadores al convertir el ejemplo en una ficha real.

Fuente autorizada del estado: la decisión identificada en el expediente correspondiente, cuando exista; el CSV conserva la propuesta y sus evidencias. Copiar «evaluado» a una ficha no crea el estado «autorizado». La aprobación de un proveedor tampoco modifica el estado canónico de v2.

Caso final. Presentar un expediente de seguridad de IA a dirección

José Manuel Hernández Agudo · Monográfico 3

Encargo al alumno

La dirección de la empresa ficticia Tech Server IIT Spain pide un expediente que permita explicar alcance, riesgos, medidas, proveedores, vigilancia, comunicaciones y recuperación. Dispones de los hechos canónicos de SYS-003 y de los supuestos adicionales identificados en las lecciones. No se permite convertir una simulación en un incidente real ni completar silenciosamente un dato que falta.

El trabajo consiste en ocho piezas: alcance y RACI; perfil de prioridades; mapa de dependencias; medidas y pruebas; proveedor; vigilancia; comunicaciones; recuperación y eficacia. Puedes usar los CSV, el cuaderno y las hojas de ampliación. No necesitas introducir datos personales ni secretos reales.

Hechos que se conservan

SYS-003 / USO-004 es el clasificador del caso. v1: 90/100 global y 9/10 críticos. v2: 94/100 global y 7/10 críticos. v2 está probada, sin autorización de despliegue. No se ha establecido la identidad o comparabilidad de las muestras ni la causa de las diferencias. T10-014 mantiene causa, daño, clasificación jurídica y obligación concreta de comunicación sin determinar. No se ha acreditado una versión implicada.

Los criterios didácticos de rendimiento no son umbrales legales de NIS2 ni de ISO. Los errores globales y críticos pueden solaparse y no se suman como nueve casos distintos. Las autorizaciones se consultan en su fuente identificada; no se infieren de una métrica, una compra o una ficha de proveedor.

Ocho decisiones que debe permitir el expediente

Pieza	Pregunta de dirección	Orientación de respuesta
H01 y RACI	¿Qué entidad, servicio, sistemas y usos examinamos y quién puede decidir?	Alcance y aplicabilidad razonados; funciones confirmadas o pendientes; delegaciones, suplencias y formación
H02	¿Por qué estas actuaciones tienen prioridad?	Escenarios, consecuencias, evidencia actual, resultados deseados y criterios de cierre
H03	¿Qué puede afectar a la cadena del servicio?	Dependencias, relaciones, límites y escenarios sin arquitectura inventada
H04	¿Qué medidas sabemos que funcionan?	Diseño y prueba separados; resultados, límites y decisión
H05	¿Puede incorporarse el proveedor para este uso?	Condiciones, evidencia, pruebas y carencias decisivas; propuesta distinta de autorización
H06	¿Qué detectamos y qué puntos ciegos quedan?	Fuentes, etapas, denominadores, prueba y capacidad de recepción y triaje
H07	¿Qué debemos comunicar y desde cuándo?	Régimen, criterio, constancia, destinatario, contenido, reloj y justificantes
H08	¿Podemos recuperar y qué mejora está comprobada?	Objetivos previos, ensayo, tiempo y punto de datos, autorización y eficacia

Modelo de informe breve a dirección

Alcance y límites. La evaluación conserva SYS-003 / USO-004 y el estado de v2. La aplicabilidad jurídica de NIS2 a la entidad requiere su expediente de actividad, tamaño, jurisdicción y disposiciones pertinentes; el uso de IA no la determina por sí solo. Los supuestos de las lecciones se utilizan para demostrar el método y no como controles implantados o incidentes reales.

Prioridades. Se propone comprobar la atribución de accesos del entorno de evaluación y la reconstrucción de las pruebas antes de ampliar conclusiones. Deben identificarse responsables, autoridad y evidencia suficiente para cada actuación. La aprobación de medidas y su supervisión se mantienen en el nivel que corresponda.

Proveedor. En C3-SUP-01 faltan condiciones suficientes de datos y coordinación urgente para el uso propuesto. La propuesta es dejar pendiente su autorización con documentación interna real. Una evaluación sintética limitada necesitaría su propia decisión y no validaría el uso real.

Vigilancia. C3-DET-01 muestra nueve registros, ocho alertas y siete avisos recibidos de diez eventos sintéticos. La entrega completa hasta guardia fue del 70 % en ese ensayo. No se ha medido la cobertura global de la empresa ni una tasa de falsas alarmas.

Comunicaciones. C3-NOT-01 tiene premisas explícitas de servicio gestionado y régimen aplicable. Su constancia se fija en el ejercicio a las 09:30 Z del 03/11/2026; la alerta de las 10:00 no reinicia el máximo general de 72 horas. Se conservan envíos simulados y su contenido. El ejemplo no resuelve la clasificación de T10-014.

Recuperación. C3-REC-01 cumple su objetivo interno de tiempo con 110 minutos, pero el punto de datos de 20 minutos supera el objetivo interno de 15. Se mantiene esa carencia y se propone comprobar alternativas y repetir el ensayo pertinente. No se afirma un número de registros perdidos sin evidencia.

Decisiones solicitadas. Confirmar funciones, límites y suplencias; priorizar las comprobaciones propuestas; asignar recursos y responsables; resolver las carencias que impidan el uso previsto; revisar evidencia de eficacia antes del cierre. Ninguna de estas propuestas crea una autorización de despliegue de v2.

Evaluación: doce preguntas con solución razonada

1. **¿Basta que la empresa utilice IA para quedar comprendida en NIS2?** No. Se documentan las reglas de ámbito y los hechos pertinentes de la entidad y servicio, junto con el régimen aplicable.

2. **¿Puede el consejo dejar de supervisar porque un AIO acepte toda la responsabilidad?** No. La asignación interna no elimina las responsabilidades atribuidas por la normativa al órgano correspondiente.

3. **¿Las cinco horas de formación propuestas son un mínimo legal?** No. Son una propuesta interna. El fundamento de ciberseguridad NIS2 y las medidas de alfabetización y competencia en IA se distinguen.

4. **¿Una huella diferente demuestra un atacante?** No. Permite identificar una diferencia de contenido respecto de la referencia examinada; origen, intención y causa requieren evidencia adicional.

5. **¿Una clave revocada en el panel demuestra rechazo de llamadas?** No por sí sola. Se comprueba el resultado efectivo, con alcance y condiciones de prueba.

6. **¿A.7 es el área general de proveedores de ISO/IEC 42001?** No. A.7 trata datos; la conexión principal de terceros está en A.10. Las correspondencias del curso se formulan funcionalmente.

7. **¿Una certificación del proveedor autoriza la integración?** No. Se examinan alcance, condiciones y evidencias propias; la autorización corresponde a la autoridad identificada.

8. **¿C3-DET-01 demuestra un 90 % de detección de extremo a extremo?** No. Se recibieron nueve registros, se generaron ocho alertas y siete avisos llegaron a guardia. El 70 % corresponde a esta última etapa respecto de los diez eventos del ensayo.

9. **¿La caída de veinte puntos en detección de críticos es el umbral del 5 % de usuarios del Reglamento 2024/2690?** No. Son magnitudes y alcances distintos. Los umbrales sectoriales requieren condiciones específicas y aplicabilidad justificada.

10. **¿La alerta temprana abre otras 72 horas para notificar?** No. En el régimen general ambas ventanas parten de la constancia del incidente significativo; se comprueban además excepciones, como servicios de confianza.

11. **¿La primera restauración de C3-REC-01 cumple todos los objetivos?** No. El tiempo con comprobaciones es 110 minutos y cumple el objetivo interno de dos horas; el punto de datos de 20 minutos no cumple el objetivo de 15.

12. **¿Puede cerrarse una mejora porque se contrató una herramienta?** La contratación acredita una actuación, no su eficacia. Se comprueba el resultado pertinente antes de sostener el cierre.

Cómo valorar el trabajo

El expediente debe ser comprensible, trazable y proporcionado al alcance. Comprueba cuatro dimensiones: fundamento de las afirmaciones; coherencia de responsabilidades y estados; calidad de las pruebas y sus límites; capacidad de decidir y dar seguimiento. Una respuesta extensa no compensa inventar una autorización, un incidente, una obligación o un resultado.

Antes de entregar, pide a otra persona que reconstruya una decisión completa utilizando solo los documentos. Si no puede localizar quién decidió, qué evidencia utilizó o qué falta por comprobar, mejora el expediente.

Matriz funcional: NIS2, NIST CSF 2.0 y SGIA

José Manuel Hernández Agudo · Monográfico 3 · 25/10/2026

Esta matriz organiza el trabajo del monográfico. Las funciones del CSF indicadas sirven para orientar la búsqueda de resultados y evidencias; cada fila admite relaciones adicionales según el contexto. No es una tabla de equivalencias jurídicas ni una declaración de cumplimiento de la organización.

Antes de utilizar una fila se documentan la aplicabilidad de la referencia, el alcance del servicio y la evidencia realmente examinada. Los ejemplos de evidencia no son una lista universal de documentos obligatorios.

Materia de NIS2	Funciones CSF relacionadas	Conexión funcional con el SGIA	Evidencia de trabajo que podría examinarse
Art. 20.1: aprobación y supervisión de medidas por el órgano de dirección	Gobernar	Liderazgo, responsabilidades, revisión y seguimiento	Decisión identificada, alcance aprobado, información revisada y seguimiento de las medidas.
Art. 20.2: formación del órgano de dirección y medidas de formación del personal en los términos de la Directiva	Gobernar, Proteger	Competencia, recursos y toma de conciencia	Necesidades por función, formación realizada y comprobación de su utilidad para las decisiones.
Art. 21.1: medidas proporcionadas y enfoque que tenga en cuenta los riesgos pertinentes	Gobernar, Identificar	Riesgos e impactos, objetivos y tratamiento	Escenarios, valoración, criterio de proporcionalidad y fundamento de la selección de medidas.
Art. 21.2.a: análisis de riesgos y políticas de seguridad de los sistemas de información	Gobernar, Identificar	Política y evaluación de riesgos	Política, alcance técnico, riesgos vinculados al servicio y decisiones de tratamiento.
Art. 21.2.b: gestión de incidentes	Detectar, Responder	Seguimiento, investigación, comunicación y mejora	Señales, cronología, hechos, medidas adoptadas, responsables y decisiones.
Art. 21.2.c: continuidad, copias de seguridad, recuperación y gestión de crisis	Proteger, Recuperar	Recursos, dependencias, cambios y continuidad del uso de IA	Configuración recuperable, objetivos justificados, ensayo y resultado de recuperación.
Art. 21.2.d: seguridad de la cadena de suministro	Gobernar, Identificar, Proteger	Relaciones con terceros y ciclo de vida	Dependencias, requisitos acordados, evidencias del proveedor, límites y pruebas de integración.
Art. 21.2.e: adquisición, desarrollo y mantenimiento seguros, con gestión y divulgación de vulnerabilidades	Identificar, Proteger, Responder	Ciclo de vida y control de cambios	Revisión del cambio, vulnerabilidades, pruebas pertinentes, decisión y seguimiento.

Materia de NIS2	Funciones CSF relacionadas	Conexión funcional con el SGIA	Evidencia de trabajo que podría examinarse
Art. 21.2.f: evaluación de la eficacia de las medidas de gestión del riesgo	Gobernar, Identificar	Evaluación del desempeño, auditoría y mejora	Método de comprobación, muestra o ensayo, resultados y tratamiento de las carencias.
Art. 21.2.g: ciberhigiene y formación en ciberseguridad	Gobernar, Proteger	Competencias y uso responsable de IA	Prácticas definidas por función, formación y comprobaciones de aplicación.
Art. 21.2.h: políticas y procedimientos sobre criptografía y cifrado cuando corresponda	Proteger	Datos, recursos y protección de la información	Necesidad justificada, configuración y gestión de claves, comprobación y límites.
Art. 21.2.i: seguridad de recursos humanos, control de accesos y gestión de activos	Gobernar, Identificar, Proteger	Responsabilidades, recursos, datos y ciclo de vida	Inventario, responsables, permisos, revisiones y cambios de acceso trazables.
Art. 21.2.j: autenticación y comunicaciones seguras en los términos aplicables	Proteger	Accesos y comunicaciones del sistema y de sus operadores	Medida elegida, adecuación al riesgo, configuración y resultado de su comprobación.
Art. 23: notificación de incidentes significativos y comunicaciones pertinentes	Gobernar, Responder	Investigación, comunicación y conservación de evidencia	Análisis de obligación, momento de conocimiento, destinatarios, plazos y actuaciones realmente realizadas.

Herramientas para concretar las conexiones

Trabajo	Herramienta del curso	Referencia jurídica o técnica	Conexión funcional con ISO/IEC 42001 y registros
Responsabilidades y formación	C3-H01A, anexo de la ficha de alcance	NIS2 art. 20; alfabetización IA por su fundamento propio	Gobierno, competencia y organización interna; RACI, decisiones y registros de formación
Evaluación de proveedores	C3-H05	NIS2 art. 21.2.d y 21.3; NIST CSF 2.0 GV.SC	Área A.10, relaciones con terceros; A.7 como complemento sobre datos; PROV-001 y registros vinculados
Clasificación y comunicaciones	C3-H07 y sus formularios	NIS2 art. 23; Reglamento 2024/2690 cuando corresponda	Área A.8, información a partes interesadas; A.9 para decisiones de uso; A.7 para datos y A.10 para terceros; INC-001 y MON-001

La herramienta de proveedores incluye las veinte preguntas con sus conexiones propuestas a GV.SC-01 a GV.SC-10. El procedimiento separa criterio general, criterios sectoriales y momentos de conocimiento. A.9 no se identifica como un catálogo completo de gestión de incidentes, ni A.7 como el área general de proveedores.

Las áreas de ISO/IEC 42001 se utilizan para organizar el trabajo, sin declarar identidad de requisitos con NIS2 o CSF ni sustituir la selección justificada de controles del SGIA. Referencias de apoyo: ficha oficial ISO y presentación institucional UNE de las áreas del anexo A.

Cómo trabajar una fila

Supuesto: el ejercicio de la lección 1 muestra dos accesos administrativos del entorno de evaluación; uno carece de responsable registrado.

1. Delimitar la afirmación. La carencia conocida afecta a la responsabilidad registrada de ese acceso, dentro del alcance del supuesto. No demuestra un ataque ni el comportamiento de todos los sistemas de la empresa.

2. Identificar el fundamento. La organización propone un criterio interno para que cada acceso administrativo tenga responsabilidad y necesidad verificadas. Si se utiliza además una referencia legal, se documenta por qué resulta aplicable al servicio y a la entidad.

3. Relacionar el trabajo. Gobernar ayuda a ordenar la responsabilidad; Identificar, a localizar el activo y sus dependencias; Proteger, a revisar y aplicar los permisos adecuados. La conexión con el SGIA debe señalar los registros pertinentes y la autoridad de decisión.

4. Comprobar el resultado. La evidencia debe mostrar qué acceso se revisó, qué se decidió y qué prueba sostiene el resultado. Una lista actualizada sin comprobar el acceso efectivo puede ser insuficiente para la conclusión que se pretenda emitir.

5. Conservar el alcance. Resolver esta carencia no acredita automáticamente la totalidad del artículo 21, el perfil objetivo completo del CSF o todo el SGIA.

Información que incorporará la matriz de trabajo

- Entidad, servicio, sistema, uso, versión y fecha de revisión.
- Fuente y aplicabilidad razonada, con las condiciones o exclusiones pertinentes.
- Resultado de ciberseguridad seleccionado y por qué importa.
- Registro existente y evidencia examinada, con su versión o localizador.
- Conclusión limitada: resultado acreditado, parcial, insuficiente o no revisado.
- Brecha, acción, autoridad, responsable confirmado y seguimiento.

Los responsables y las autorizaciones se vincularán a la estructura real o a los datos expresos del supuesto didáctico. Los códigos del curso no se transforman por sí solos en una fuente autorizada del estado.

Fuentes

Directiva (UE) 2022/2555.

NIST CSF 2.0.

ENISA: guía técnica de implementación de NIS2.

Las conexiones con el SGIA reutilizan los procesos y registros trabajados en el curso y se concretan en H01-H08. La evaluación de una fila conserva alcance, fuente, evidencia, límites y autoridad.

Glosario y códigos para navegar por el monográfico

Término	Significado en el curso
SGIA	Sistema de gestión de la inteligencia artificial
NIS2 / SRI 2	Directiva (UE) 2022/2555; su aplicabilidad se analiza por entidad y servicio
CSF	Marco de ciberseguridad de NIST; organiza resultados y no otorga certificación de NIST
Perfil actual / objetivo	Situación respecto de resultados examinados / resultados que se pretende alcanzar
RACI	Asignación interna de realización, decisión, consulta e información
AIO	Nombre interno propuesto para coordinación del gobierno de IA; no cargo creado por art. 20 NIS2
CISO	Función de seguridad; sus tareas y autoridad se concretan en la organización
SSOT	Autoridad definida sobre un dato y alcance; no exige una sola base física ni que gane la copia más reciente
RTO	Objetivo de tiempo de recuperación, con inicio y condiciones definidos
RPO	Objetivo de punto de recuperación de datos, distinto del tiempo de restauración
Incidente significativo	Categoría que se evalúa con criterios y régimen pertinentes; no todo fallo de IA
T_constancia	Momento en que la entidad tiene constancia del incidente significativo; no fecha elegida al aprobar un informe

Código	Registro o referencia
SYS-003 / USO-004	Clasificador y uso del caso canónico
R-001	Registro de riesgos
IMP-001	Registro de impactos
FD-001	Información y trazabilidad de datos
SUP-001	Supervisión
PROV-001	Proveedores y dependencias
CAM-001	Cambios y decisiones vinculadas
MON-001	Seguimiento, señales y resultados
INC-001	Incidentes, investigación y comunicaciones

Código	Registro o referencia
T10-014	Episodio del curso con causa, daño, clasificación y obligación sin establecer
H01-H08	Herramientas locales de este monográfico; no sustituyen los registros anteriores

R-001 e IMP-001 identifican registros del curso. No se cambian identificadores de referencias de un caso por parecerse al nombre de un registro. Se conserva siempre el alcance de la información y la autoridad de su estado.

Fuentes oficiales y cómo utilizarlas

Las lecciones distinguen ley, reglamento, norma de gestión, marco técnico, contrato y criterio docente. Cada obligación se conecta con su ámbito, sujeto y hechos pertinentes. Las correspondencias organizan el trabajo; no declaran identidad de todos los requisitos.

1. Directiva (UE) 2022/2555, publicación del DOUE. Ámbito, definiciones, gobierno, medidas y comunicaciones. Artículos 20, 21 y 23 son centrales para este monográfico.
2. Reglamento de Ejecución (UE) 2024/2690. Requisitos y criterios concretos para las entidades de su ámbito. Artículos 3, 4 y 10 se trabajan en los supuestos con condiciones expresas.
3. NIST CSF 2.0. Marco de resultados de ciberseguridad.
4. CSF 2.0 en español, alojado por NIST. Apoyo de lectura y terminología.
5. NIST SP 1301. Perfiles organizativos.
6. NIST SP 1302. Niveles del CSF y su contexto.
7. NIST SP 1305. Capacidad de gestión de cadena de suministro y definición de requisitos.
8. Preguntas frecuentes oficiales NIST. Uso, certificación y relación con otros marcos.
9. ENISA, guía técnica NIS2 de 2025. Recomendaciones y ejemplos dentro del alcance al que se dirige; se distingue de obligación general.
10. ISO/IEC 42001:2023, ficha oficial y material institucional UNE sobre sus áreas de control. Apoyan el mapa funcional del SGIA.
11. Reglamento (UE) 2026/1744, artículo 1.5. Redacción modificada del artículo 4 del AI Act utilizada para explicar alfabetización en IA.
12. Comisión Europea, comunicación de 8 de julio de 2026 sobre transposición. Hito fechado del procedimiento; no reemplaza comprobar disposiciones aplicables al expediente de la entidad.

Las fuentes son dinámicas. Al completar un expediente real se documentan versión y fecha de la disposición aplicable y sus cambios. Los ejemplos internos de tiempos, porcentajes de ensayo y carga de estudio no se convierten en mínimos legales.

Ampliación de respuestas · hoja 1

Completa con hechos, evidencias, límites y decisiones identificadas.

Lección o herramienta y continuación de respuesta

Lección o herramienta y continuación de respuesta

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.

Ampliación de respuestas · hoja 2

Completa con hechos, evidencias, límites y decisiones identificadas.

Lección o herramienta y continuación de respuesta

Lección o herramienta y continuación de respuesta

Si el texto no cabe visible, utiliza las hojas de ampliación al final del cuaderno.
Comprueba la impresión: el texto desplazado dentro de un campo puede no imprimirse.