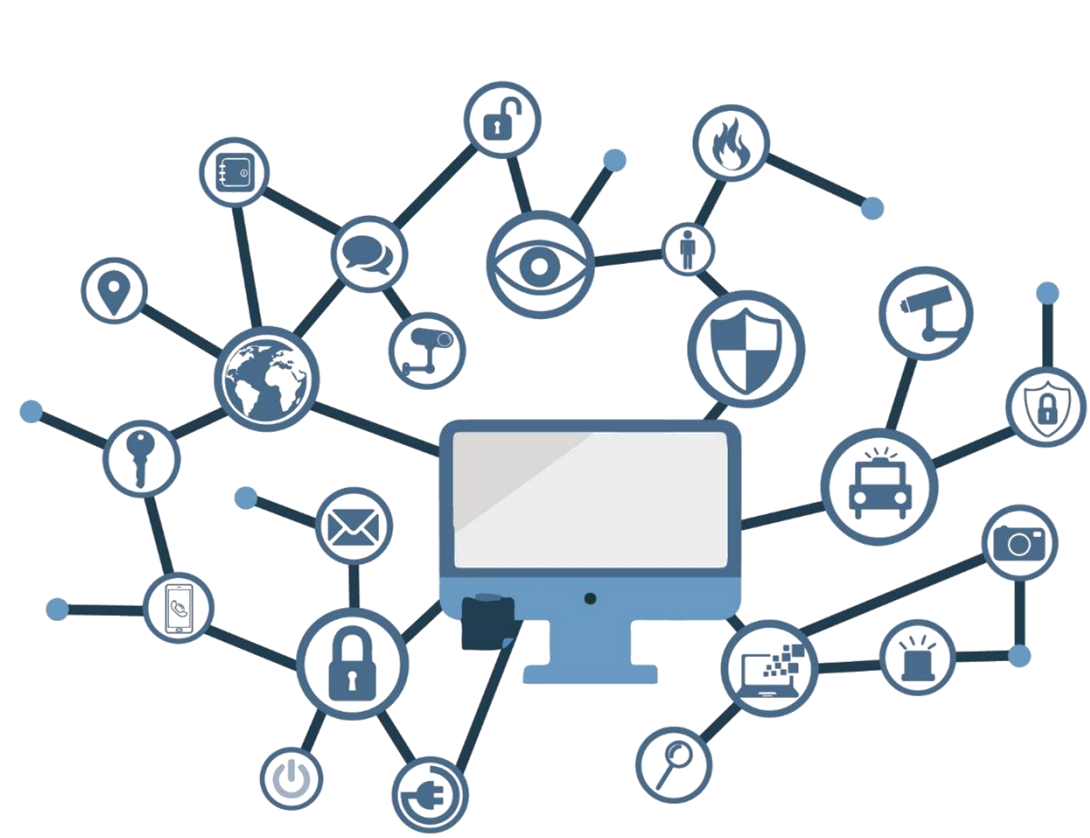
centro criptológico nacional

Guía de Seguridad de las TIC
Anexo D CCN-STIC 2010

Plantilla del Informe Técnico de Monitorización de Productos en la Nube (CICLON)



Abril 2026

Edita:

centro criptológico nacional

Fecha de Edición: abril de 2026

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.04.24 11:11:31 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. Introducción

Este documento es una plantilla de referencia para la redacción del Informe Técnico de Monitorización (MTR) de un servicio en la nube en el marco de la Evaluación de Productos en la Nube (CICLON). La plantilla establece el contenido mínimo que debe incluirse en el MTR.

Su contenido deberá adaptarse y completarse en función de la tipología, alcance y características del producto o servicio objeto de monitorización.

1.1 Información del Informe Técnico de Monitorización

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

LABORATORIO EVALUADOR	
Nombre del Laboratorio	
ID del Laboratorio *Identificador único asignado al laboratorio de evaluación.*	
Dirección *Dependencias donde se realiza la monitorización.*	
Email de contacto	
Teléfono de contacto	
METADATOS DEL INFORME	
Versión MTR *Versión del esquema del informe de monitorización (p. ej. 1.0.0).*	
Número de la iteración *Número de la iteración pertinente a este informe.*	
Fecha *Fecha de la realización de la monitorización.*	
ID de informe *Identificador único de este informe (UUID).*	
ID informe anterior *Referencia al informe de la iteración anterior (UUID).*	
Código de expediente *Identificador único del expediente proporcionado por el CPSTIC.*	

INFORMACIÓN DEL TOE	
Nombre del producto	
Taxonomía del producto *Según CCN-STIC 140. Ej.: HERRAMIENTAS ANTI-VIRUS / EPP (ENDPOINT PROTECTION PLATFORM)* En caso de no aplicar, indicar: NO APLICA [1] [2]	
Solicitante	
Email del solicitante	
Dirección del solicitante	
Fabricante	
Referencia declaración de seguridad *Ref. al documento DS del producto evaluado.*	
Referencia ETR *Referencia al informe técnico de evaluación (ETR).*	

[1] En caso de que la declaración de seguridad no cumpla estrictamente con todos los requisitos marcados en los anexos definidos por los responsables del CPSTIC en la CCN-STIC-140.
[2] La declaración de seguridad deberá ser aprobada por parte de los responsables del CPSTIC.

2. Veredicto de la monitorización

El evaluador deberá indicar en el Informe Técnico de Monitorización (MTR) el Porcentaje de Garantía de Monitorización (PGM), de conformidad con lo establecido en la metodología CICLON [CCN-STIC-2010].

Dicho porcentaje únicamente será válido cuando se cumplan de forma concurrente las siguientes condiciones:

1. La funcionalidad de seguridad del TOE cumple lo establecido en la Declaración de Seguridad y el TOE no es vulnerable a ninguno de los ataques descritos en [CCN-ITC-003].
2. Todas las actividades de evaluación definidas en la metodología han obtenido el veredicto de **PASA**.
3. No se ha superado el tiempo máximo de evaluación y las evidencias aportadas cumplen los requisitos esperados.

Si cualquiera de estas condiciones no se cumple, el veredicto de la evaluación y monitorización será **FALLA** y, en consecuencia, el **Porcentaje de Garantía de Monitorización (PGM)** asignado será **0**, con independencia del porcentaje que pudiera haberse calculado.

3. Análisis de conformidad

3.1 Análisis de librerías de terceros

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Procesamiento del Fichero de Librerías (SBOM). El evaluador deberá documentar el proceso de análisis del fichero SBOM proporcionado por el fabricante, indicando las herramientas utilizadas, las fuentes de vulnerabilidades consultadas y las evidencias obtenidas.
b) Categorización de vulnerabilidades. El evaluador deberá clasificar cada vulnerabilidad pública identificada conforme a los rangos de criticidad definidos por CVSS v4.0, de acuerdo con el siguiente criterio:
    1. Crítica: Desde 9.0 hasta 10.0
    2. Alta: Desde 7.0 hasta 8.9
    3. Media: Desde 4.0 hasta 6.9
    4. Baja: Desde 0.1 hasta 3.9
c) Listado de las no conformidades detectadas, indicando para cada una de ellas su descripción, justificación y, en su caso, su impacto sobre la monitorización. Se deberá prestar especial atención a la existencia de vulnerabilidades de criticidad crítica, cuya presencia implica un valor C = 0 en el cálculo del PGM1.
d) Porcentaje de Garantía resultante de esta etapa (PGM1). Valor calculado por el evaluador mediante la fórmula establecida en la metodología, con indicación explícita de los valores utilizados en el cálculo.
e) Resultados del análisis. El evaluador deberá registrar los resultados obtenidos conforme a la siguiente estructura, incluyendo, cuando aplique, la comparativa respecto a la iteración anterior de la monitorización:

RESULTADOS PGM1	Valor Actual	Iteración Anterior	Delta
Puntuación *Puntuación global del PGM1 en esta iteración.*			
Vulnerabilidades CVE			
CVE Crítica (C) *Número de vulnerabilidades de criticidad Crítica.*			
CVE Alta (H) *Número de vulnerabilidades de criticidad Alta.*			
CVE Media (M) *Número de vulnerabilidades de criticidad Media.*			
CVE Baja (L)			

Número de vulnerabilidades de criticidad Baja.			
CVE Total (T) *Total de vulnerabilidades detectadas.*			

3.2 Verificación de los componentes de integración

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Verificación de componentes de integración. El evaluador deberá verificar que los componentes de integración que se encuentran declarados en la Declaración de Seguridad estén evaluados bajo la Metodología CICLON.
b) Porcentaje de Garantía resultante de esta etapa (PGM2). Valor calculado por el evaluador mediante la fórmula establecida en la metodología, con indicación explícita de los valores utilizados en el cálculo.
c) Resultados del análisis. El evaluador deberá registrar los resultados obtenidos conforme a la siguiente estructura, incluyendo, cuando aplique, la comparativa respecto a la iteración anterior de la monitorización:

RESULTADOS PGM2	Valor Actual	Iteración Anterior	Delta
Puntuación *Puntuación global del PGM2 en esta iteración.*			
Componente integrado n (repetir este bloque tantas veces como componentes integrados tenga el TOE)			
PGC (Componente n) *Porcentaje de Garantía Compuesto (PGC) del componente n.*			
RFS (Componente n) *Número de Requisitos Fundamentales de Seguridad (RFS) que son implementados por el componente n.*			
Componente n *Número de componentes externos que contribuyen a implementar funcionalidad de seguridad.*			
R *Número total de requisitos definidos en la declaración de seguridad.*			

d) Listado de componentes integrados evaluados. El evaluador deberá verificar y documentar cada componente externo declarado en la Declaración de

Seguridad, indicando su estado de evaluación bajo la Metodología CICLON, su Porcentaje de Garantía Compuesto (PGC), el número de requisitos fundamentales de seguridad que implementa y la vigencia de su certificación. Se deberá prestar especial atención a los componentes cuya evaluación haya caducado (estado EXPIRED), ya que su inclusión en el cálculo del PGM2 puede invalidar el resultado de esta etapa.

Componente	Taxonomía	Fabricante	CPSTIC ID	PGC (%)	RFS	Estado	Fecha Eval.	Caducidad
Auth-Module	XXXX	XXXX	CIC-2025-81	91,5 %	8	**VALIDO**	15/08/2025	15/08/2027
HSM	XXXX	XXXX	CIC-2026-69	94,0 %	6	**EXPIRADO**	10/03/2025	10/03/2026

3.3 Revisión de las certificaciones aplicables al proveedor de la plataforma nube

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Certificados aplicables. El evaluador deberá comprobar la vigencia de los diferentes certificados aplicables entregados por el fabricante.
b) Porcentaje de Garantía resultante de esta etapa (PGM3). Valor calculado por el evaluador mediante la fórmula establecida en la metodología, con indicación explícita de los valores utilizados en el cálculo.
c) Resultados del análisis. El evaluador deberá registrar los resultados obtenidos conforme a la siguiente estructura, incluyendo, cuando aplique, la comparativa respecto a la iteración anterior de la monitorización:

RESULTADOS PGM3	Valor Actual	Iteración Anterior	Delta
Puntuación *Puntuación global del PGM3 en esta iteración.*			
Certificaciones aplicables (repetir este bloque tantas veces como certificaciones aplicables tenga el TOE)			
ENS *Certificado Esquema Nacional de Seguridad (ENS)*			

d) Listado de certificaciones aplicables al proveedor de la plataforma nube. El evaluador deberá verificar y documentar cada certificación declarada en la Declaración de Seguridad, indicando el tipo de certificación, su nivel, fecha de emisión y expiración, así como su alcance.

Certificación	Nivel	Fecha Emisión	Caducidad	Alcance
ENS	Alto	15/08/2026	15/08/2028	Infraestructura tecnológica en territorio español

4. Cálculo del porcentaje de garantía de monitorización (PGM)

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Porcentajes de Garantía Parciales. El evaluador deberá registrar los Porcentajes de Garantía obtenidos en cada una de las etapas anteriores de la fase de monitorización, indicando explícitamente los valores de PGM1, PGM2 y PGM3, así como los factores de peso asociados a cada uno de ellos.

b) Porcentaje de Garantía de Monitorización (PGM). Valor calculado por el evaluador mediante la fórmula establecida en la Metodología de Evaluación de Productos en la Nube [CCN-STIC-2010], con indicación explícita de los valores utilizados en el cálculo.

RESULTADOS PGM	Valor Actual	Iteración Anterior	Delta
Puntuación PGM *Puntuación global del PGM en esta iteración.*			
Puntuación PGM1 *Puntuación global del PGM en esta iteración.*			
Puntuación PGM2 *Puntuación global del PGM en esta iteración.*			
Puntuación PGM3 *Puntuación global del PGM en esta iteración.*			

5. Cálculo del porcentaje de garantía compuesto (PGC)

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Porcentaje de Garantía Compuesto (PGC). Valor calculado por el evaluador mediante la fórmula establecida en la Metodología de Evaluación de Productos en la Nube [CCN-STIC-2010].

RESULTADOS PGC	Valor Actual	Iteración Anterior	Delta
Puntuación PGC *Puntuación global del PGC en esta iteración.*			
Puntuación PGE *Puntuación global del PGE*			
Puntuación PGM *Puntuación global del PGM en esta iteración.*			

6. Referencias

[CC]	Common Criteria for Information Technology Security Evaluation. Se debe considerar su última versión aprobada y publicada en la web del Organismo de Certificación (https://oc.ccn.cni.es).
[CCN-STIC-2010]	Metodología de Evaluación de Productos en la Nube (CICLON).
Anexo A [CCN-STIC-2010]	Plantilla para la Declaración de Seguridad de la Evaluación de Productos en la Nube (CICLON).
Anexo B [CCN-STIC-2010]	Plantilla para el Documento de Arquitectura del Servicio de la Evaluación de Productos en la Nube (CICLON).
Anexo C [CCN-STIC-2010]	Plantilla del Informe Técnico de Evaluación de Productos en la Nube (CICLON).
Anexo D [CCN-STIC-2010]	Plantilla del Informe Técnico de monitorización de Productos en la Nube (CICLON).
CCN-ITC-003	Instrucción Técnica de Evaluación de seguridad en entornos web y nube.
FOR-CIC-001	Formulario de solicitud de evaluación de Productos en la Nube (CICLON).
PO-006	Procedimiento de acreditación de laboratorios.
PO-CIC-005	Procedimiento de certificación de productos en la nube.
PO-CIC-010	Procedimiento de autorización de laboratorios para evaluaciones CICLON.
SBOM CycloneDX	Estándar para composición software.

7. Acrónimos

CCN	Centro Criptológico Nacional
CD	Comprobación Directa
CI	Comprobación Indirecta
CICLON	Certificación Iterativa Cloud Nacional
CPSTIC	Catálogo de Productos y Servicios STIC
DAS	Documento de Arquitectura del Servicio
DIAS	Diagrama de Arquitectura del Servicio
DS	Declaración de Seguridad
ENS	Esquema Nacional de Seguridad
ENECSTI	Esquema Nacional de Evaluación y Certificación de Seguridad TIC
ETR	Informe Técnico de Evaluación
EUCC	Esquema Europeo de Certificación (European Cybersecurity Certification Scheme)
ITC	Instrucción Técnica
MTR	Informe Técnico de Monitorización
PGC	Porcentaje de Garantía Compuesto
PGE	Porcentaje de Garantía de Evaluación
PGM	Porcentaje de Garantía de Monitorización
SBOM	*Software Bill of Materials*
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TOE	Producto objeto de evaluación (*Target of Evaluation*)
WAF	*Web Application Firewall*