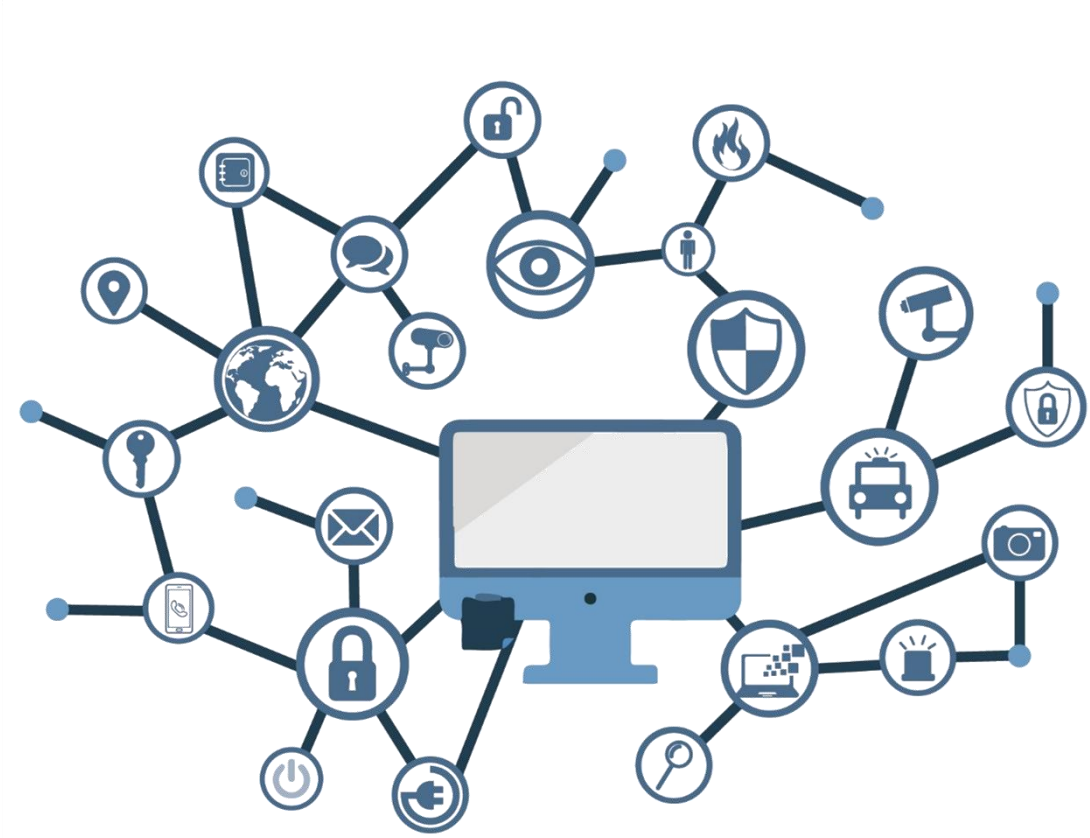
centro criptológico nacional

ICT Security Guide
Annex D CCN-STIC 2010

Cloud Product Monitoring Technical Report Template (CICLON)



April 2026

Edited by:

Edition date: april 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.12 12:20:30 +02'00'

LIMITATION OF LIABILITY

The present document is provided in accordance with the terms set forth herein, expressly rejecting any type of implied warranty related thereto. Under no circumstances shall the National Cryptologic Center be liable for any direct, indirect, incidental, or extraordinary damages arising from the use of the information and software provided herein, even if advised of such possibility.

LEGAL NOTICE

INDEX

1. Introduction

This document is a reference template for drafting the Monitoring Technical Report (MTR) of a cloud service within the framework of the Cloud Product Evaluation (CICLON). The template establishes the minimum content that must be included in the MTR.

Its content must be adapted and completed according to the typology, scope, and characteristics of the product or service being monitored.

1.1 Monitoring Technical Report Information

The information that must be included in this section is, at a minimum, the following:

LABORATORY EVALUATOR	
Laboratory Name	
Laboratory ID *Unique identifier assigned to the evaluation laboratory.*	
Address *Premises where monitoring is carried out.*	
Email Contact	
Phone Number Contact	
REPORT METADATA	
MTR Version *Version of the monitoring report schema (p.e.g. 1.0.0).*	
Iteration number *Number of the iteration relevant to this report.*	
Date *Date the monitoring was performed.*	
Unique identifier of this report *Unique identifier of this report (UUID).*	
Previous report ID *Reference to the report of the previous iteration (UUID).*	
Dossier code *Unique identifier of the file provided by CPSTIC.*	
TOE INFORMATION	

Product name	
Product taxonomy *According to CCN-STIC 140. E.g.: ANTI-VIRUS TOOLS / EPP (ENDPOINT PROTECTION PLATFORM)* If not applicable, indicate: NOT APPLICABLE [1] [2]	
Applicant	
Applicant´s email address	
Applicant´s address	
Manufacturer	
Security target reference *Ref. to the document of the evaluated product*	
ETR reference *Reference to the evaluation technical report (ETR).*	

[1] In case the security target does not strictly comply with all the marked requirements in the annexes defined by the team responsible for the CPSTIC in the CCN-STIC-140.
[2] The security target must be approved by the team responsible for the CPSTIC.

2. Monitoring Verdict

The evaluator must indicate the Monitoring Assurance Score (PGM) in the Monitoring Technical Report (MTR), in accordance with the CICLON methodology [CCN-STIC-2010].

This score will only be valid when the following conditions are met concurrently:

1. The TOE's security functionality complies with the Security Target (ST), and the TOE is not vulnerable to any of the attacks described in [CCN-ITC-003].
2. All evaluation activities defined in the methodology have received a **PASS** verdict.
3. The maximum evaluation time has not been exceeded, and the evidence provided meets the expected requirements.

If any of these conditions are not met, the evaluation and monitoring verdict will be **FAIL**, and consequently, the assigned Monitoring Assurance Score (PGM) will be **0**, regardless of any score that may have been calculated.

3. Compliance Analysis

3.1 Analysis of third-party libraries

The information that must be included in this section is, at a minimum, the following:

a) Processing of the Library File (SBOM). The evaluator must document the analysis process of the SBOM file provided by the manufacturer, indicating the tools used, the vulnerability sources consulted, and the evidence obtained.

b) Vulnerability categorization. The evaluator must classify each identified public vulnerability according to the criticality ranges defined by CVSS v4.0, in accordance with the following criteria:
   1. Critical: From 9.0 to 10.0
   2. High: From 7.0 to 8.9
   3. Medium: From 4.0 to 6.9
   4. Low: From 0.1 to 3.9

c) List of detected non-conformities, indicating for each one its description, justification, and, where applicable, its impact on monitoring. Special attention must be paid to the existence of critical vulnerabilities, whose presence implies a value of C = 0 in the calculation of PGM_1.

d) Assurance Score resulting from this stage (PGM_1). Value calculated by the evaluator using the formula established in the methodology, with explicit indication of the values used in the calculation.

e) Results of the analysis. The evaluator must record the results obtained according to the following structure, including, where applicable, a comparison with the previous monitoring iteration:

PGM_1 RESULTS	Current Value	Previous Iteration	Delta
Score *Overall score of PGM_1 in this iteration.*			
CVE Vulnerabilities			
Critical CVE (C) *Number of critical criticality vulnerabilities.*			
High CVE (H) *Number of high criticality vulnerabilities.*			
Medium CVE (M) *Number of medium criticality vulnerabilities.*			
Low CVE (L)			

Number of low criticality vulnerabilities.			
Total CVE (T) *Total vulnerabilities detected.*			

3.2 Integration components verification

The information that must be included in this section is, at a minimum, the following:

a) Verification of integration components. The evaluator must verify that the integration components declared in the Security Target are evaluated using the CICLON Methodology.

b) Assurance Score resulting from this stage (PGM_2). Value calculated by the evaluator using the formula established in the methodology, with explicit indication of the values used in the calculation.

c) Analysis results. The evaluator must record the results obtained according to the following structure, including, where applicable, a comparison with the previous monitoring iteration:

PGM_2 RESULTS	Current Value	Previous Iteration	Delta
Score *Overall score of PGM_2 in this iteration.*			
Integrated component n (repeat this block as many times as the TOE has integrated components)			
PGC (Component n) *Composite Assurance Score (PGC) of component n.*			
RFS (Component n) *Number of Fundamental Security Requirements (RFS) implemented by component n.*			
Component n *Number of external components that contribute to implementing security functionality.*			
R *Total number of requirements defined in the security target.*			

d) List of evaluated integrated components. The evaluator must verify and document each external component declared in the Security Target, indicating its evaluation status under the CICLON Methodology, its Composite Assurance Score (PGC), the number of fundamental security requirements it

implements, and the validity of its certification. Special attention should be paid to components whose evaluation has expired (EXPIRED status), as their inclusion in the PGM_2 calculation may invalidate the result of this stage.

Component	Taxonomy	Manufacturer	CPSTIC ID	PGC (%)	RFS	Status	Eval. Date	Expiration
Auth-Module	XXXX	XXXX	CIC-2025-81	91,5 %	8	**VALID**	15/08/2025	15/08/2027
HSM	XXXX	XXXX	CIC-2026-69	94,0 %	6	**EXPIRED**	10/03/2025	10/03/2026

3.3 Review of the certifications applicable to the cloud platform provider

The information that must be included in this section is, at a minimum, the following:

a) Applicable certificates. The evaluator must check the validity of the different applicable certificates provided by the manufacturer.

b) Assurance Score resulting from this stage (PGM_3). Value calculated by the evaluator using the formula established in the methodology, with explicit indication of the values used in the calculation.

c) Analysis results. The evaluator must record the results obtained according to the following structure, including, when applicable, the comparison with the previous monitoring iteration:

PGM_3 RESULTS	Current Value	Previous Iteration	Delta
Score *Overall score of PMG_3 in this iteration.*			
Applicable certifications (repeat this block as many times as the TOE has applicable certifications)			
ENS *National Security Scheme Certificate (ENS)*			

d) List of certifications applicable to the cloud platform provider. The evaluator must verify and document each certification declared in the Security Target, indicating the type of certification, its level, date of issue and expiration, as well as its scope.

Certification	Level	Emission Date	Expiry	Scope
ENS	High	15/08/2026	15/08/2028	Technological infrastructure in Spanish territory

4. Calculation of monitoring assurance score (PGM)

The information that must be included in this section is, at a minimum, the following:

a) Partial Assurance Score. The evaluator must record the Assurance Scores obtained in each of the previous stages of the monitoring phase, explicitly indicating the values of PGM_1, PGM_2 and PGM_3, as well as the weight factors associated with each of them.

b) Monitoring Assurance Score (PGM). Value calculated by the evaluator using the formula established in the Cloud Product Evaluation Methodology [CCN-STIC-2010], with explicit indication of the values used in the calculation.

PGM RESULTS	Current Value	Previous Iteration	Delta
PGM Score *Overall PGM score in this iteration.*			
PGM_1 Score *Overall PGM_1 score in this iteration.*			
PGM_2 Score *Overall PGM_2 score in this iteration.*			
PGM_3 Score *Overall PGM_3 score in this iteration.*			

5. Calculation of the composite assurance score (PGC)

The information that must be included in this section is, at a minimum, the following:

a) Composite Assurance Score (PGC). Value calculated by the evaluator using the formula established in the Cloud Product Evaluation Methodology [CCN-STIC-2010.

RESULTADOS PGC	Current Value	Previous Iteration	Delta
PGC Score *Overall PGC score in this iteration.*			
PGE Score *PGE overall score.*			
PGM Score *Overall PGM score in this iteration.*			

6. References

[CC]	Common Criteria for Information Technology Security Evaluation. The latest version approved and published on the Certification Body's website (https://oc.ccn.cni.es) must be considered.
[CCN-STIC-2010]	Metodología de Evaluación de Productos en la Nube (*Cloud Product Evaluation Methodology*) (CICLON).
Anexo A [CCN-STIC-2010]	Plantilla para la Declaración de Seguridad de la Evaluación de Productos en la Nube (*Template for the Cloud Product Evaluation Methodology*) (CICLON).
Anexo B [CCN-STIC-2010]	Plantilla para el Documento de Arquitectura del Servicio de la Evaluación de Productos en la Nube (*Template for the Cloud Product Evaluation Service Architecture Document*) (CICLON).
Anexo C [CCN-STIC-2010]	Plantilla del Informe Técnico de Evaluación de Productos en la Nube (*Cloud Product Evaluation Technical Report Template*) (CICLON).
Anexo D [CCN-STIC-2010]	Plantilla del Informe Técnico de monitorización de Productos en la Nube (*Cloud Product Monitoring Technical Report Template*) (CICLON).
CCN-ITC-003	Instrucción Técnica de Evaluación de seguridad en entornos web y nube (*Technical Instruction for Security Evaluations in Web and Cloud Environments*).
FOR-CIC-001	Formulario de solicitud de evaluación de Productos en la Nube (*Application form for Cloud Products Evaluations*) (CICLON).
PO-006	Procedimiento de acreditación de laboratorios (*Laboratory Accreditation Procedure*).
PO-CIC-005	Procedimiento de certificación de productos en la nube (*Cloud Product Certification Procedure*)
PO-CIC-010	Procedimiento de autorización de laboratorios para evaluaciones CICLON (*Laboratory authorization procedure for CICLON evaluations*).
SBOM CycloneDX	Estándar para composición software (*Standard for software composition*)

7. Acronyms

CCN	Centro Criptológico Nacional (*National Cryptology Center*)
CICLON	Certificación Iterativa Cloud Nacional (*National Cloud Iterative Certification*)
CPSTIC	Catálogo de Productos y Servicios STIC (*Catalog of Products and Services STIC*)
DAS	Documento de Arquitectura de Servicio (*Service Architecture Document*)
DIAS	Diagrama de Arquitectura del Servicio (*Service Arquitecture Diagram*)
DV	Direct Verification
ENECSTI	Esquema Nacional de Evaluación y Certificación de Seguridad TIC (*National Scheme for Evaluation and Certification of ICT Security*)
ENS	Esquema Nacional de Seguridad (*Security National Scheme*)
ETR	Informe Técnico de Evaluación (*Evaluation Technical Report*)
EUCC	Esquema Europeo de Certificación (*European Cybersecurity Certification Scheme*)
ITC	Instrucción Técnica Complementaria (*Supplementary Technical Instruction*)
IV	Indirect Verification
MTR	Informe Técnico de Monitorización (*Monitoring Technical Report*)
PGC	Porcentaje de Garantía Compuesto (*Composite Assurance Score*)
PGE	Porcentaje de Garantía de Evaluación (*Evaluation Assurance Score*)
PGM	Porcentaje de Garantía de Monitorización (*Monitoring Assurance Score*)
SBOM	Software Bill of Materials

ST	Security Target
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones (*Security of the Information and Communication Technology*)
TOE	Producto objeto de evaluación (*Target of Evaluation*)
WAF	Web Application Firewall