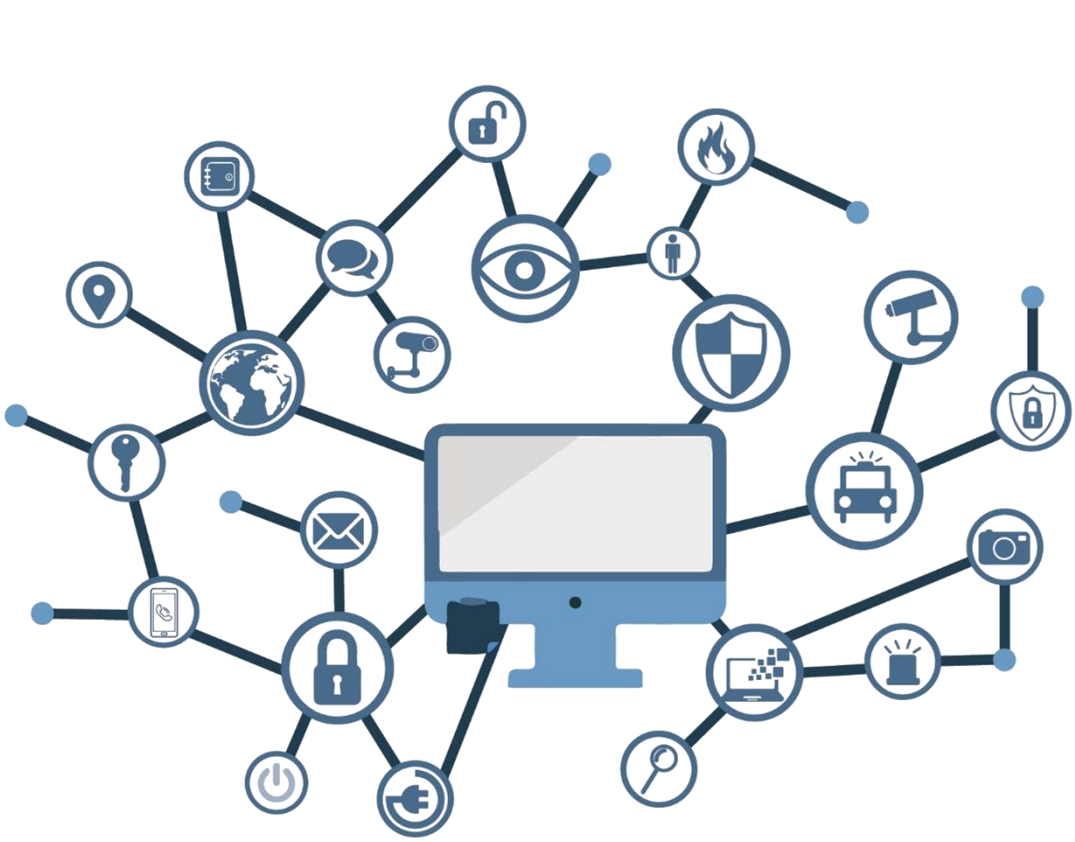
centro criptológico nacional

ICT Security Guide
Annex C CCN-STIC 2010

Cloud Product Evaluation Technical Report Template (CICLON)



April 2026

Edited by:
centro criptológico nacional

Edition date: april 2026

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

Without the written authorization of the National Cryptologic Center, the partial or total reproduction of this document by any means or procedure, including photocopying and computer processing, and the distribution of copies through public rental or loan, are strictly prohibited under the penalties established by the law.

INDEX

1. Introduction

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

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

1.1 Evaluation Technical Report information

ETR reference	Unique identifier given by the laboratory
ETR version	Document version
Evaluation Laboratory	Laboratory Name Address of the dependencies where the evaluation is carried out
Author or authors	Name of the ETR Author
Revised by	Name of the ETR Revisor
Approved by	Name of the ETR responsible
Date	ETR modification date
Dossier Code	Unique identifier given by CPSTIC
Product taxonomy according CCN- STIC 140	E.g.- ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM) or NOT APPLICABLE[1] [2]

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

1.2 TOE Applicant information

Applicant Details (Name and Address)	
Applicant Contact Details (Contact name and e-mail)	
Developer Details (Name and Address)	
TOE Name	

2. TOE description

The evaluator must indicate that the information included in this section has been obtained from the Security Target.

2.1 TOE functional description

A clear and concise description of the TOE will be included, identifying in natural language its main components and all the security functions that constitute the TOE.

2.2 Security functions inventory

The security functions gathered in the Security Target must be described and classified according to their functionality. Each security function must be assigned a unique identifier, which will be used consistently throughout the report to reference that function.

3. Operational environment

The evaluator must indicate that the information included in this section has been obtained through the Security Target.

3.1 Description of the operational environment

The operational environment required to enable the execution of the product must be specified.

3.2 Operational environment assumptions

The assumptions regarding the operational environment in which the product will be operated must be included. Each assumption will be assigned a unique identifier, which will be used consistently throughout the report.

4. Executive summary of the evaluation

This section will include an executive summary of the evaluation, highlighting the most relevant aspects of its development and the results obtained. In particular, the non-conformities identified, observation reports issued, evidence received, and significant milestones achieved during the evaluation process should be reflected.

The information should be presented in chronological order, to facilitate understanding the sequence of activities carried out and the evolution of the evaluation.

The purpose of this section is to offer a concise and organized overview of the evaluation process, allowing for understanding, at a high level, its development and the most relevant facts associated with it.

5. Verdict of the evaluation

The evaluator must indicate the Evaluation Assurance Score (PGE) in the Evaluation Technical Report (ETR), in accordance with the CLICLON 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, 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 verdict will be **FAIL**, and consequently, the assigned **Evaluation Assurance Score (PGE)** will be **0**, regardless of any score that may have been calculated.

6. Access and configuration of the testing environment

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

a) Identification of the evaluator(s) responsible for carrying out this activity.
b) Date or period of execution of the activity.
c) Description of the test environment provided for the evaluation, indicating whether it is a production environment or an equivalent pre-production environment, as well as the conditions of access to the TOE, including, where applicable, the existence of access via WAF.
d) Description of the configuration applied to the TOE during the evaluation, with explicit reference to the configuration(s) defined in the Security Target, as well as identification of any non-conformities detected in relation to access to and configuration of the test environment.
e) Result of the tasks performed by the evaluator at this stage, including, at least:
    1. Verification that the applicant has provided the required access to the test environment.
    2. Verification that the product can be configured according to the configuration(s) described in the Security Target.
    3. Verification of the absence of non-conformities in accessing and configuring the test environment.
f) Evaluation Assurance Score corresponding to this stage, indicating the formula applied, the values assigned to the variables used, and the justification for the result obtained.
g) Effort dedicated by the evaluator to accessing the test environment and configuring the TOE according to the instructions contained in the Security Target.

7. Compliance Analysis

7.1 Security Target Analysis

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

a) Identification of the evaluator(s) responsible for carrying out this activity.
b) Date or period of execution of the activity.
c) Reference to the identifier and version of the Security Target being evaluated.
d) Results of the tasks performed by the evaluator in this stage, including the justification for the verdict assigned to each task. In particular, a record must be kept of the checks carried out on:
    1. The presence of the elements described in [Annex A CCN-STIC-2010].
    2. The identification of the TOE name
    3. Verification of the use of the validated version of the Security Target by the team responsible for the CPSTIC.
    4. The clarity and sufficiency of the TOE description.
    5. The delimitation between the TOE and its operational environment, as well as a description of the support that the latter provides for its execution.
    6. The coherence of the security problem, including assets, assumptions, threats, and security functions.
    7. The level of detail with which the security functions implemented in the TOE are described.
    8. The absence of non-conformities related to the analysis of the Security Target.
e) List of the non-conformities detected, indicating for each its description, justification, and, where applicable, its impact on the evaluation.
f) Evaluation Assurance Score corresponding to this stage, including details of the formula applied, the values used for its variables, and the justification for the result obtained.
g) Effort dedicated by the evaluator to the analysis of the Security Target.

7.2 Analysis of the Service Architecture Document

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

a) Identification of the evaluator(s) responsible for this activity.
b) Date or period of execution of the activity.
c) Reference to the identifier and version of the Service Architecture Document (DAS) analyzed.
d) Results of the checks performed on the DAS, including, at least:
    1. Verification that the document is complete and corresponds to the evaluated TOE.

2. Verification that the DAS defines the possibility of accessing the TOE without using the WAF.
3. Verification of the correct delimitation between the elements that form part of the TOE and those that belong to the operational environment, as well as the adequate description of the support that the latter provides for the execution of the TOE.
4. Verification of the absence of non-conformities related to the Service Architecture Document.

e) List of non-conformities detected, indicating for each its description, justification, and, where applicable, its impact on the evaluation.
f) Evaluator's conclusion on the sufficiency and suitability of the DAS for the evaluation.
g) Effort dedicated by the evaluator to the analysis of the DAS.

7.3 Functional tests

This section will record the results of the functional tests performed on the security functions defined in the Security Target (ST), in accordance with the CICLON methodology.

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

a) Identification of the evaluator(s) responsible for this activity.
b) Date or period of test execution.
c) Identification of the security functions tested, indicating for each whether its verification was performed using Direct Verification (DV) or Indirect Verification (IV), as well as the justification for the designation criterion (DV or IV) applied.
d) Detailed information on each test performed, including its objective, scenario, procedure, expected results, results obtained, and conclusion.
e) List of non-conformities detected and their association with the corresponding tests, security functions, or evidence.
f) Effort dedicated to the execution and analysis of the functional tests.

For each function tested, the evaluator must complete the following "Test Case" template:

Test code:	**(E.g.- PF_0xx)**
Security function tested:	**Evaluator:**
	Test objective:
Test scenario:	
Context	

Type of check: DV / IV	**Type of test:** Standard / Manipulation (tampering) / Elusion (bypassing)
Procedure	
Expected results	
Results obtained	
Conclusion and verdict:	

Example:

Test code:	
Security function tested: Protecting the web service against SQL injection attempts in HTTP/HTTPS input parameters	**Evaluator:** PF_WAF_001 **Test objective:** Verify, through Direct Verification (DV), that the TOE blocks SQL injection attempts targeting application input parameters and that this protection cannot be circumvented through variations in encoding, normalization, or location of the input vector.
Test scenario: Pre-production environment equivalent to production. Corporate web application published through a WAF in blocking mode, with TLS termination on the front end and routing to the application and database back end.	
Context	
Type of check: DV	**Type of test:** Bypassing
Procedure	
1. Verify that the injection protection policy is enabled in the WAF for GET and POST methods, as well as for query parameters, forms, and JSON bodies. 2. Send legitimate reference requests to confirm normal service behavior and establish a functional baseline. 3. Execute a set of controlled malicious requests using SQL injection patterns on different application entry points. 4. Repeat the test using semantically equivalent variants aimed at evading the security mechanism, including encoding changes, alternative representations of reserved characters, higher case and upper-case variations, insertion of spaces or separators, and sending the vector through different entry points of the request.	

5. Check if the WAF blocks requests before they reach the backend, and additionally verify in the WAF, application, and database logs whether any of the sent requests were partially or fully processed.
6. Record the triggered rules, the event identifier, the timestamp, the request origin, and the affected resource.

Expected results

- The TOE must identify and block malicious requests aimed at exploiting SQL injection.
- Protection must be maintained against evasion variants based on encoding, normalization, or alternative vector placement.
- Blocked requests must not reach the application logic or generate query execution in the backend.
- The event must be logged with sufficient detail for traceability and subsequent analysis.
- There must be no data leakage, revealing error messages, or alteration of the service's functional behavior

Results obtained

The reference requests were processed successfully. The WAF blocked the direct SQL injection variants sent in query parameters and HTTP forms. However, during the bypass test, an equivalent variant introduced in a nested attribute of the JSON body was not blocked by the TOE and reached the backend application, which returned a controlled validation error.

[Include evidence obtained during the procedure]

The review of evidence showed that the WAF logged the request as an anomalous event but did not apply the blocking action because deep inspection of the JSON body was not enabled for that resource. There was no evidence of successful execution of the malicious query or data exfiltration, but there was a partial bypass of the declared preventative mechanism.

Conclusion and verdict:

The security function is considered partially implemented. The Test of Entries (TOE) demonstrates the ability to detect and block direct SQL injection attempts, but the bypass test reveals evasion scenarios in JSON inputs not inspected to the same depth as conventional parameters. Consequently, the test result is **FAIL**, as a way to bypass the declared security mechanism has been demonstrated.

7.4 Cryptographic communications analysis

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

a) Identification of the evaluator(s) responsible for this activity.
b) Date or period of test execution.

c) Identification and definition of communication channels. The evaluator must document the external and internal communication channels related to the TOE that are defined and identified in the Security Target, verifying that this identification is unambiguous and complete.

d) Consistency between documents. The evaluator must record the result of the consistency verification between what is established in the Security Statement and what is declared in the Service Architecture Document, indicating any discrepancies detected, if any.

e) Results of the cryptographic analysis. Detailed description of the analysis process carried out, including the tools used, the channels analyzed, the protocols and algorithms identified, the key sizes, the modes of operation, and the evidence obtained. It must be expressly stated whether the identified cryptographic mechanisms are classified as Recommended, Not Recommended (NR), or Legacy (L) as of the date of the assessment.

f) List of detected non-conformities, indicating for each its description, justification, and, where applicable, its impact on the assessment.

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

h) Effort dedicated to the execution of the cryptographic communication analysis.

8. TOE Penetration tests

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

a) Identification of the evaluator(s) responsible for this activity.
b) Date or period of test execution.
c) Penetration testing. The evaluator must perform, at a minimum, the set of tests described in the Technical Instruction for Security Evaluation in Web and Cloud Environments [CCN-ITC-003].
d) List of detected non-conformities, indicating for each its description, justification, and, where applicable, its impact on the assessment. It must be expressly verified that no non-conformity originated from a successful attack.
e) Effort dedicated to performing the penetration tests.

For each penetration test performed, the evaluator must complete the following "Test Case" template:

Test code:	(E.g.- PT_0xx)
Associated Vulnerability of [CCN-ITC-003]:	**Evaluator:**
	Test objective:
Attack Scenario:	
Procedure	
Expected results	
Results obtained	
Conclusion and verdict:	

9. Calculation of the evaluation assurance score (PGE)

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 evaluation phase, explicitly indicating the values of PGE_1, PGE_3, and PGE_5, as well as the weighting factors associated with each of them (w_1, w_3, w_5).

b) Evaluation Assurance Score (PGE). 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.

10. Safe Operating Procedure (PES) considerations

This section should contain considerations regarding the safe operation of the TOE.

The evaluator must document all safe operation considerations identified during the evaluation that should be incorporated into the Safe Operating Procedure (PES) guide.

These considerations must be necessary for the TOE to fulfill all the safety functions defined in its Safety Target.

11. 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).
Annex 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).
Annex 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).
Annex C [CCN-STIC-2010]	Plantilla del Informe Técnico de Evaluación de Productos en la Nube (*Cloud Product Evaluation Technical Report Template*) (CICLON).
Annex 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 Assessment*) (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*).

12. 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	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 (*Compound 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	Target of Evaluation
WAF	Web Application Firewall