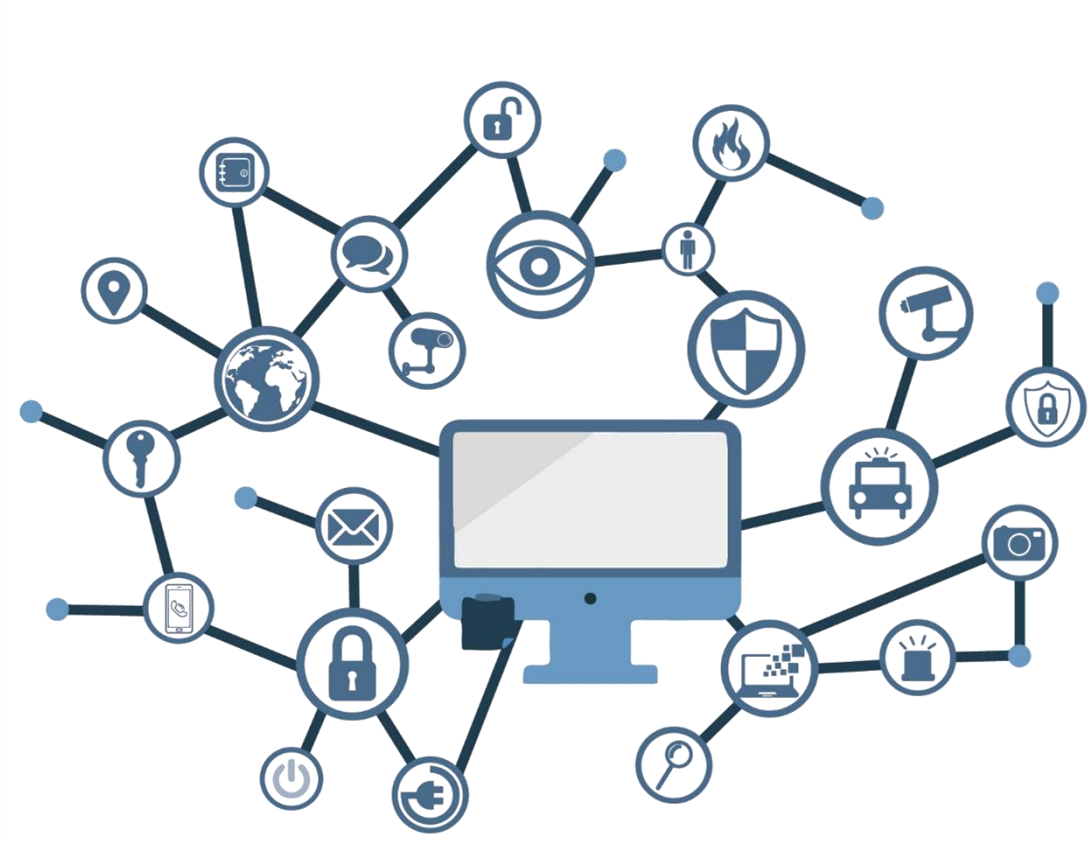
centro criptológico nacional

ICT Security Guide
Annex A CCN-STIC 2010

Template for the Security Target of Cloud Products Evaluation (CICLON)



March 2026

Edited by:

Edition date: march 2026

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.12 12:18:06 +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

Version Control

Version	Comment	Date
1.0	Initial version	03/2026

INDEX

1 INTRODUCTION

This document is a reference template for drafting the Security Target of a cloud service for the Evaluation of Cloud Products (CICLON).

1.1 APPLICANT, TOE AND EVALUATION INFORMATION

Applicant data	
Developer data	
TOE name	
Evaluation type	CICLON version 1
Estimated effort (evaluator-days)	
Guidance documents and versions (optional)	
Taxonomy according to CCN-STIC-140	

1.2 METHODOLOGY AND EVALUATION CRITERIA

CCN-STIC-2010	Evaluation of Cloud Products (CICLON) Methodology

2 TOE DESCRIPTION

2.1 TOE FUNCTIONAL DESCRIPTION

A clear and concise description of the cloud-based TOE shall be included, using natural language, describing its main components and the main security functions that are subject to the evaluation.

2.2 IDENTIFICATION OF THE TOE SECURE USE, INSTALLATION AND CONFIGURATION GUIDES

A table shall be included identifying the operation and configuration guides (when required) that allow the TOE to be operated in its evaluated configuration. These guides shall be accessible to the consumers of the cloud service.

The table shall include at least the document type, name, and a cryptographic hash of the document.

Document's type	Document' name	HASH (SHA256)

If no secure operation and configuration guides are available, this section shall clearly indicate that such guides do not exist and explain the reason.

2.3 TOE USAGE DESCRIPTION

If any specific TOE parameter must be configured for its use, this section shall be used to describe it.

If the service provides the necessary functionality to meet its security objective without requiring any parameter configuration, this situation shall be explicitly stated.

3 OPERATIONAL ENVIRONMENT

3.1 OPERATIONAL ENVIRONMENT DESCRIPTION

The Security Target shall specify the operational environment required to enable the execution of the cloud service.

The environment shall indicate the cloud platform provider where the TOE is deployed and all the required components for the TOE to provide its service.

A diagram showing a high-level view of the TOE environment shall be included (this diagram may be a simplified version of the Service Architecture Design document, DAS).

3.2 INTEGRATED COMPONENTS (OPTIONAL)

In cases where a security requirement is covered by another evaluated product or a product under evaluation, such product shall be described in this section as an Integrated Component, describing the characteristics of the integration and indicating which security requirements it covers (e.g. ADM.1).

4 SECURITY PROBLEM DEFINITION

4.1 OPERATIONAL ENVIRONMENT ASSUMPTIONS

The Security Target shall include assumptions regarding the environment in which the product will be executed, defining the scope of the evaluation. Depending on the declared assumptions about the operational environment, the TOE may be limited in its ability to provide some of the declared security functionalities.

Possible assumptions about the operational environment may relate to physical security measures, procedural, personnel security, or logical security applied in the operational environment.

Each assumption about the operational environment shall be stated according to the following table.

Assumption	Description

4.2 ASSETS TO PROTECT

The Security Target shall describe the assets protected by the TOE security functions. The security properties protected for each asset shall be specified (confidentiality, integrity, availability, authenticity and/or traceability).

To protect the listed assets, the product may make use of other information which shall itself be considered an asset.

Each sensitive asset to protect shall be identified according to the following table:

Asset	Description	Security Dimensions

4.3 THREAT DESCRIPTIONS

The Security Target shall describe the threats mitigated by the TOE security functions. A threat may be characterized by the following elements:

a) An actor (authorized user, administrator, malicious user, external attacker, etc.).
b) The adverse action performed by the actor (data injection, malicious access, information extraction, etc.).
c) The asset or assets affected by the adverse action.

Each threat shall be identified according to the following table:

Threat	Description	Assets

5 SECURITY FUNCTIONAL REQUIREMENTS

The Security Target shall include the specific security functions provided by the cloud-deployed product. These functions shall be described in natural language.

The specification shall be complete enough for the evaluator to clearly understand how the functionality has been implemented, in other words, a high-level description of how the TOE provides the specific security functionality shall be given.

Security functions shall be present in the intended usage mode of the TOE and within the evaluation scope, i.e. functions that are not evaluated shall not be described.

Since the Security Target is a public document, the manufacturer may choose not to include sensitive or proprietary information. In such cases, the expected implementation details about the sensitive security functions shall be included in Annex B of the CCN-STIC-2010 Service Architecture Design (DAS) and referenced from the Security Target. In any case, a consumer of the evaluated service must be able to understand the scope of the cloud product evaluation by reading the Security Target; therefore, the laboratory shall verify that the information provided in the Security Target allows for the identification of the certified security functionalities.

The verification method for each requirement is defined according to the following criteria:

a) **Indirect Verification (IV):** applicable when the laboratory cannot directly verify the security function.
b) **Direct Verification (DV):** applicable when the laboratory can perform the security function tests on the TOE, including functional and penetration testing.
c) **Integration (Int.):** applicable when the security function is covered by a component defined in the operational environment as an integrated element and has been configured by the manufacturer.

Each requirement shall indicate how it will be tested according to the following table:

5.1 SF. SECURITY FUNCTION NAME

The title of this section shall indicate the name of the corresponding Security Function. There shall be as many sections as security functions.

Requirement ID	Verification method	Description

6 REFERENCES

This section shall reference all documents used for the analysis and justification of the different requirements.

[CCN-STIC-2010]	Process definition of Cloud Product Evaluation (CICLON)
[CCN-STIC-140-X]	Reference Taxonomy for ICT Security Services

7 ACRONYMS

CCN	Centro Criptológico Nacional (*National Cryptologic Center*)
CNI	Centro Nacional de Inteligencia (*National Intelligence Center*)
DAS	Diseño Arquitectura del Servicio (*Service Architecture Design*)
ENS	Esquema Nacional de Seguridad (*National Security Scheme*)
ICT	Information and Communication Technologies
LINCE	Certificación Nacional Esencial de Seguridad (*National Essential Security Certification*)
MCF	Módulo Revisión de Código Fuente (*Source Code Review Module*)
MEB	Módulo de Evaluación Biométrica (*Biometric Evaluation Module*)
MEC	Módulo de Evaluación Criptográfica (*Cryptographic Evaluation Module*)
ST	Security Target - Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación (*Security of Information and Communication Technology)*
TOE	Target Of Evaluation – Objeto a evaluar