Autoridad Nacional de Certificación de la Ciberseguridad

centro criptológico nacional

ANCC-PO-01

Annual report

March 2026
Version 1

MINISTERIO DE DEFENSA

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained therein, expressly rejecting any type of implied warranty that may be found related. In no event can the National Cryptologic Center be held liable for direct, indirect, incidental or extraordinary damages arising from the use of the information and software indicated even when it is warned of such possibility.

LEGAL NOTICE

It is strictly prohibited, without the written authorization of the National Cryptologic Center, under the sanctions established by law, the partial or total reproduction of this document by any means or procedure, including reprography and computer processing, and the distribution of copies thereof by public rent or loan.

COURTESY TRANSLATION NOTICE

This document is provided solely as a courtesy translation. This translation has been generated using automated tools with minimal human supervision. In the event of any discrepancy, ambiguity, or conflict between this translation and the original Spanish version, the original Spanish version text shall prevail and shall be deemed the only official, authoritative, and legally binding version.

VERSION CONTROL

Version	Comments
1.0	Initial version

INDEX

1. INTRODUCTION

1. This procedure defines the timetable, expected content and responsibilities for the preparation of the annual report of the National Certification Authority **(NCCA),** in accordance with **Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and to the certification of cybersecurity of information and communication technologies** (hereinafter **CSA**) **[CSA]**.

2. CONTENT AND STRUCTURE OF THE REPORT

2. The **NCCA** shall prepare an annual activity report, which shall be submitted within the first quarter (**T1**) of the following calendar year. This report shall cover the full year immediately preceding and shall be submitted to **the European Commission** and to the European Cybersecurity Certification Group **(ECCG)** in compliance with Article 58 of the **[CSA] and in accordance with the format and template provided by ENISA and approved by the ECCG.**

3. The report shall consider at least the following activities:

a) **Activities under Article 58(7)(b) of the [CSA].**

This section provides an overview of the supervision activities carried out by the **NCCA** on manufacturers or suppliers established in its territory carrying out *self-assessment*. It includes statistics on the actions carried out, the cases processed and the trends observed with respect to previous years, together with any incidents identified and the measures taken. Where, depending on the applicable scheme, these activities do not apply, the section shall expressly indicate this.

b) **Activities under Article 58(7)(c) of the [CSA].**

This section summarizes the assistance and support provided by the **NCCA** to the national accreditation body in the supervision of conformity assessment bodies. It includes information such as the number of **CABs** covered, the cooperation mechanisms established, the type of technical support provided and the follow-up activities carried out. It also provides an analysis of observed trends and observations or improvements resulting from these activities.

c) **Activities under Article 58(7)(d) of the [CSA].**

This section describes the supervision activities carried out by **NCCA** on the public bodies referred to in Article 56(5). It summarizes the number of supervised entities, the types of actions carried out and the main findings detected. It includes statistics on incidents or deviations observed, the follow-up actions applied and the status of the cases processed, along with relevant trends and recommendations for improvement.

d) **Activities carried out under Article 58(8) of the [CSA].**

This section summarizes the exercise of the powers provided for in Article 58(8), which include requests for information, audits or investigations, corrective measures, access to facilities, withdrawal of certificates or imposition of sanctions. It presents data on the number and type of these actions, together with the results

obtained, the challenges faced and the lessons learned, as well as the planned improvements for subsequent periods.

e) **Notification and associated supervision activities, as provided for in European certification schemes.**

This section contains information on notifications from accredited or authorized conformity assessment bodies, as well as data related to certificates issued under the supervision of the **NCCA** at the various assurance levels. It includes statistics on notifications, active **CABs** and issued or active certificates, along with an analysis of relevant trends and observations. If no activity has been carried out in the reference period, it will be expressly indicated as not applicable.

3. PREPARATION AND REVIEW PROCESS

4. The preparation of the annual report follows a timetable defined each year in order to ensure its timely completion. The overall process is coordinated by the head of the **NCCA** unit **(JAN),** with the **NCCA** technical staff **(TA)** collecting data and drafting content, as detailed below:

a) **Start** — At the beginning of each year (usually during the first week of January), the **JAN** begins the process of preparing the annual report. The **JAN** issues an internal communication (e.g. by e-mail or by a meeting) to the relevant **TAs** to initiate data collection, indicating the scope of the information required and setting preliminary deadlines.

b) **Data collection** — **TAs** collect all necessary data relating to previous year's activities. This includes extracting quantitative data from the National Cybersecurity Certification Authority information system (**SGA)** (such as the number of oversight actions, support actions, and authorization decisions recorded), reviewing internal activity records and, where necessary, conducting brief interviews or consultations with staff members involved in activities related to letters (b), (c) and (d). The data collection phase should be largely completed by mid-January, so that both statistical data and qualitative inputs are available (e.g. relevant issues or identified good practices).

c) **Drafting** — Based on the data collected, **TAs** prepare a draft annual report. The draft is organized according to the prescribed structure (supervision, support to **ENAC**, authorizations and peer evaluations). **TAs** collect quantitative results (including tables or figures, if applicable) and write analytical commentary for each section, addressing trend analysis and any recommendations. The full draft should be ready for review by the end of January or at the beginning of February.

d) **Review** — The **JAN** reviews the draft report in detail. This review checks the accuracy of the data, the clarity of the explanations and the relevance of any conclusions or recommendations. The **JAN** makes comments or requests revisions from **TAs** as needed. This review and feedback cycle should take place during February, allowing sufficient time to fill any gaps or errors.

e) **Final Review and Approval** — **TAs** incorporate **JAN** comments and produce a revised final draft. Once all comments have been addressed, the **JAN** makes a final review and formally approves the content of the report. The goal is for final approval to take place before the end of February, ensuring that the report is ready for submission within the first quarter.

4. COMPLETION AND PRESENTATION

5. Once adopted, the annual report is finalized for submission. The **JAN** ensures that the approved report is transmitted securely to the **European Commission** and the **ECCG** (e.g. via secure official email or through the designated platform). This presentation should be made by the end of the first quarter. Where possible, confirmation of receipt will be obtained from the recipients, and a copy of the submitted report (and any acknowledgment of receipt) will be filed in the **SGA** or in the records of the Authority. By sharing the report with **ENISA** and the **ECCG**, the **NCCA** contributes to the overall objective of harmonization between Member States, as the findings and outstanding trends will serve as a basis for discussions and best practices within the European Cybersecurity Certification Group.

5. REFERENCES

ACCCB	Accreditation of certification bodies for EUCC (https://certification.enisa.europa.eu/publications/accreditation-cbs-eucc_en)
ACCITSEF	Accreditation of ITSEF for EUCC (https://certification.enisa.europa.eu/publications/accreditation-itsefs-eucc_en)
AUTH	Authorisation of certification bodies and ITSEF for the EUCC scheme (https://certification.enisa.europa.eu/publications/eucc-guidelines-authorisation-cabs_en)
CSA	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies, and repealing Regulation (EU) No 526/2013 (http://data.europa.eu/eli/reg/2019/881/oj)
CSA-E1	Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services (http://data.europa.eu/eli/reg/2025/37/oj)
EUCC	Implementing Regulation (EU) 2024/482 of the 31 January 2024 Commission laying down detailed rules for the implementation of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European criteria-based cybersecurity certification scheme common (http://data.europa.eu/eli/reg_impl/2024/482/oj)
LPAC	Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (https://www.boe.es/eli/es/l/2015/10/01/39/con)
NOTIF	Commission Implementing Regulation (EU) 2024/3143 of 18 December 2024 laying down the circumstances, formats and procedures for notification in accordance with Article 61(5) of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cybersecurity) and certification of cybersecurity of information and communication technologies (http://data.europa.eu/eli/reg_impl/2024/3143/oj)
VULMD	Guidelines on Vulnerability Management and Disclosure (https://certification.enisa.europa.eu/publications/eucc-guidelines-vulnerability-management-and-disclosure-and-eccg-opinion_en)

6. ACRONYMS

NCCA	National Cybersecurity Certification Authority
CCN	National Cryptologic Center
EC	European Commission
CSIRT	Computer Security Incident Response Teams
ENAC	National Accreditation Body
ENISA	European Union Agency for Cybersecurity
EUCC	European cybersecurity certification scheme based on common criteria
ECCG	European Cybersecurity Certification Group
ITSEF	Information Technology Security Evaluation Facility
JAN	Head of the NCCA unit
CB	Certification Body
CAB	Conformity assessment body
CSA	Cybersecurity Regulations
SED	Secretary of State Director of the CCN
SGA	Information System of the National Cybersecurity Certification Authority
TA	Technical staff attached to the NCCA
ICT	Information and Communication Technologies
EU	European Union
VPA	Voluntary periodic audits
WNCCA	Website of the National Cybersecurity Certification Authority