Adaptation to National Security Scheme

E-Government Security Tools

Over two years have passed since the enforcement of ***Royal Decree 3/2010**, of 8 January 2010, regulating the National Security Scheme for E-Government*, a development of the provisions in Article 42 of Law 11/2007. The **National Security Scheme (ENS)**, drafted in cooperation with all Public Administrations, contains the basic principles and minimum requirements for an adequate protection of information, aimed at establishing the security policy in the use of electronic media within the scope of the aforementioned Law.

After all this time, information and service security in Public Administration continues to be a strategic aspect to e-government. In fact, it is considered in the **Spanish Cybersecurity Strategy**, now in progress, being one of its goals and a course of action to ensure ENS is fully implemented.

Adaptation to ENS involves addressing the following issues:

- Drafting and approval of a security policy, including definition of roles and allocation of responsibilities.
- System classification according to the importance of the information handled and the services provided.
- Risk analysis, including assessment of existing security measures.
- Drafting and approval of Statement of Applicability of the measures in Annex 2 to ENS.
- Drafting of an adaptation plan for security improvement, based on the failures identified, including estimated development schedule.
- Implementation, execution and monitoring of security measures through ongoing security management.
- Security audit in two years' time, resulting in relevant improvement actions.

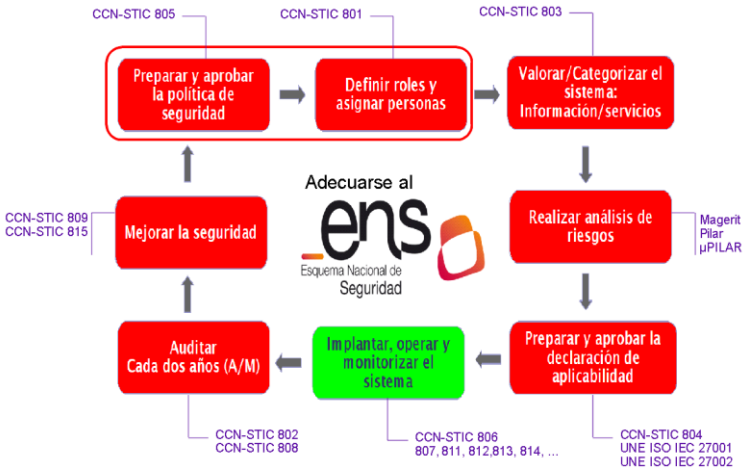

Figure: Key actions for adaptation to ENS.

Also, when it comes to adapting to ENS, **the items below will be of help:**

- Special tools and guidelines.
- Common infrastructures and services.
- Existing standards.
- Security incident reports.
- Certified products.
- Enquiries.
- Training.

Over the past two years, there has been intense uninterrupted activity for the development of **support tools for adaptation to ENS**. These tools include the **CCN-STIC guides** envisaged in Article 29 of Royal Decree 3/2010 and available at the CCN-CERT website[i]. They were developed by the National Cryptology Centre, with the support of the Ministry of Finance and Public Administration (MINHAP). The following CCN-STIC guides have been released so far:

- 800 – Glossary of ENS Terms and Abbreviations.
- 801 – ENS Heads and Functions.
- 802 – ENS Audits.

- 803 – ENS System Evaluation.
- 804 – ENS Implementation Measures.
- 805 – Information Security Policy.
- 806 – ENS Adaptation Plan.
- 807 – Cryptology Used in ENS.
- 808 – ENS Compliance Testing.
- 809 – ENS Statement of Compliance.
- 810 – CERT/CSIRT Creation Guidelines.
- 812 – Internet Application and Environment Security.
- 813 – Certified Components.
- 814 – Email Security.
- 815 – ENS Indicators and Measurements.
- 817 – ENS Security Incident Management Criteria.

Work is currently being done to add **new guides** for guidance in such issues as security operational procedures, denial-of-service attacks or cloud computing, among others. Another line of work has to do with identifying **high-impact, low-cost ENS measures** and giving guidance for faster security improvement.

These guides are supplemented by risk analysis and management tools, including the MAGERIT V.2 method (V.3 will be released soon), and PILAR and μPILAR, containing the ENS protection profile.

In addition, in accordance to Articles 36 and 37 of Royal Decree 3/2010, the **CCN-CERT response services to security incidents** are already available. They are supplemented by the **early alert services in the SARA Network.**

Also, there are the services of the National IT Security Evaluation and Certification Scheme Certification Board[ii], regarding lab accreditation and IT security product certification.

Moreover, progress is being made in the improvement of the **FAQ series on ENS**, based on the answering of questions on application.

Finally, there are the **training** efforts on ICT security, in both **traditional** classroom and **distance** modes: **STIC courses** from CCN, MINHAP and INAP (classroom), and introductory courses to ENS (20 hours) and the PILAR tool (10 hours) in the private or public areas of the CCN-CERT website (distance learning).

[i] https://www.ccn-cert.cni.es/, https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2420&Itemid=211&lang=es

[ii] http://www.oc.ccn.cni.es/