

## Monitoring of the adaptation to the National Security Framework and the National Interoperability Framework

### Advances in the adaptation to the NSF and the NIF by the Public Administrations

During 2013 and the first quarter of 2014 the **progress of adaptation to the National Security Framework (NSF; ENS in Spanish) and the National Interoperability Framework (NIF; ENI in Spanish) has been monitored**. This monitoring was agreed by the Standing Committee of the Higher Council for E-Government in October 2012. It has been gradually extended to other public authorities, especially to the Autonomous Communities, through the eGovernment Sectoral Committee. The participation in this monitoring is made on a voluntary basis and it has been implemented by successive waves of questionnaires in February, May, September and December 2013 and March 2014. The questionnaire reviews the progress of the different chapters of the frameworks, helps to identify areas of greatest difficulty, and invites to send proposals and suggestions.

The Ministry of Finance and Public Administrations, responsible for both frameworks, implemented the monitoring through the Directorate General for Administrative Modernisation, Procedures and Promotion of Electronic Government, in the case of ENS in cooperation with the National Cryptologic Centre of the National Intelligence Center.

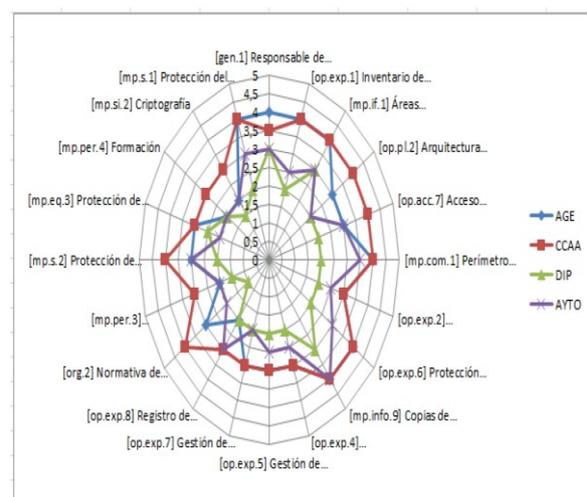
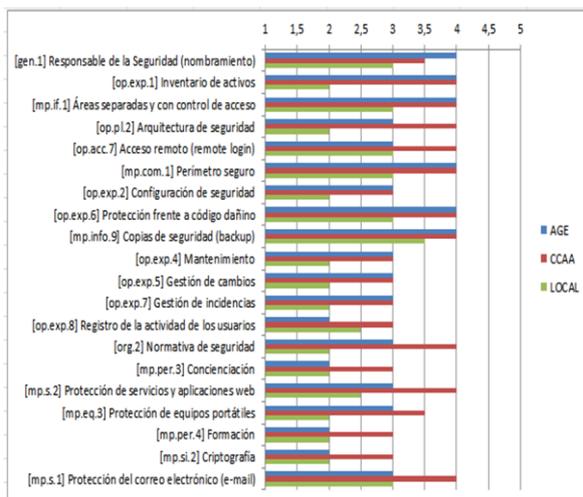
This document provides information on the progress of adaptation to the NSF and the NIF after the questionnaire of March 2014. It should be noted that the effort to adapt to the two frameworks, NSF and NIF, is performed under conditions that pose a significant effort for the public administrations, due to the limitation and, often, reduced financial and human resources.

## National Security Framework

The monitoring of the progress of adaptation to the NSF has been supported by a tool available on the CCN-CERT Portal<sup>1</sup>. The intensity of participation is remarkable, especially of the Central Government, followed by the autonomous communities, taking into account that the participation is voluntary:

	2013				2014
	febrero	mayo	septiembre	diciembre	marzo
Administración General del Estado	64	69	77	78	88
Comunidades Autónomas	5	26	28	30	30
Ayuntamientos	2	12	13	14	22
Diputaciones		5	6	6	9
<b>Total</b>	<b>71</b>	<b>112</b>	<b>124</b>	<b>128</b>	<b>149</b>

The following charts provide a comparative overview based on a subset of security measures considered especially relevant.



Traditional aspects of security are quite advanced: protection of facilities and infrastructure, protection of personal data, identification of users, backups; progress is also observed in formal aspects such as the establishment of a security policy and the nomination of a security responsible, among other measures.

It should be emphasized that it is essential that **there is an adaptation plan and a responsible for security; that the categorization of systems is done; and that a risk analysis is performed**. While in terms of more specific recommendations it is desirable to address certain measures which affect mostly aspects of security related to the situation on the ground: promote governance aspects and documentation including measures such like *Authorization Process* and *Security Architecture*; implement the CCN-STIC guidelines laid down in Article 29 of the NSF in particular in relation to the *Security Configuration* and *Protection of web applications*; apply *Configuration Management*, *Maintenance* and *Change Management*; and measures relating to the activity as the *Register of user activity*, and *Intrusion Detection* and *System metrics*; without neglecting *Awareness* and *Training*.

From now on, the **INES Project (National Security State Report)**, developed by the CCN-CERT, with support from the Ministry of Finance and Public Administrations, will provide the public administrations a faster and intuitive knowledge of their level of alignment with the NSF and the of state of security of their systems, as stated in Article 35 of the NSF.

In addition, among the tools to adapt to the NSF, the CCN-STIC guides include 25 guides (800 series)<sup>ii</sup> about policies, procedures to implement the measures outlined in the NSF within a larger set of 200 guides. Also the Risk Analysis Tool called PILAR is in the CCN-CERT portal available for download, together with an online course about the tool.

In addition, the **SAT (Early Warning Service)** is a service made available to all public authorities and companies of strategic interest that began in 2009. In these five years, 57 public and private organizations (65 probes) have joined the service and

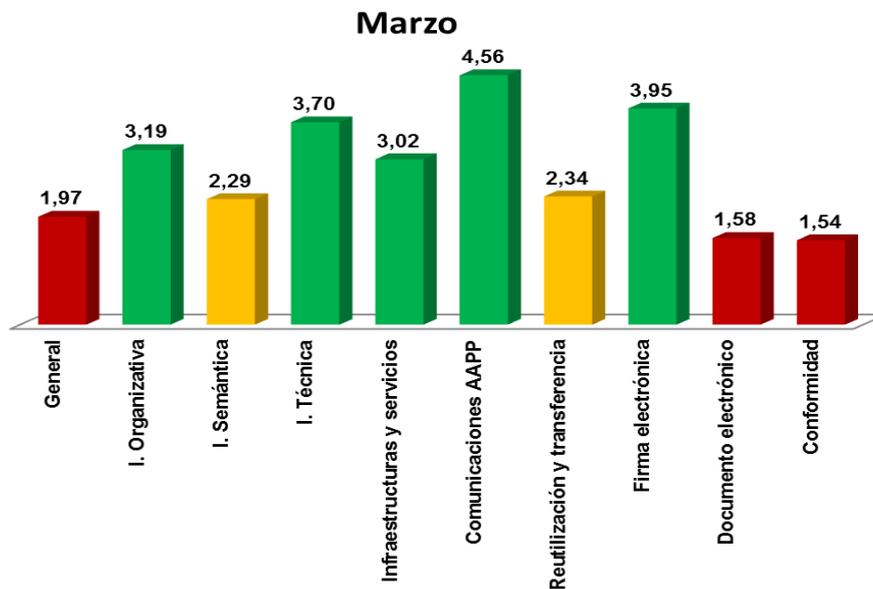
enjoyed the benefits that are offered to protect their systems and to contain and eliminate cyber threats. In fact, through this service, a total of 6,350 cybersecurity incidents were managed, representing a 89% increase over the previous year. For 2014 the implementation of this service will be extended, including local councils, and their performance will be improved, including new sources. Along with this, and as a key point, the sharing rules and Indicators of Compromise (IOC) for better management of an attack will be addressed.

Other tools available include **LUCIA (Unified Incident Coordination Listing and Threats)** for incident management and **CARMEN for analyzing search logs and traffic anomalies**.

### ***National Interoperability Framework***

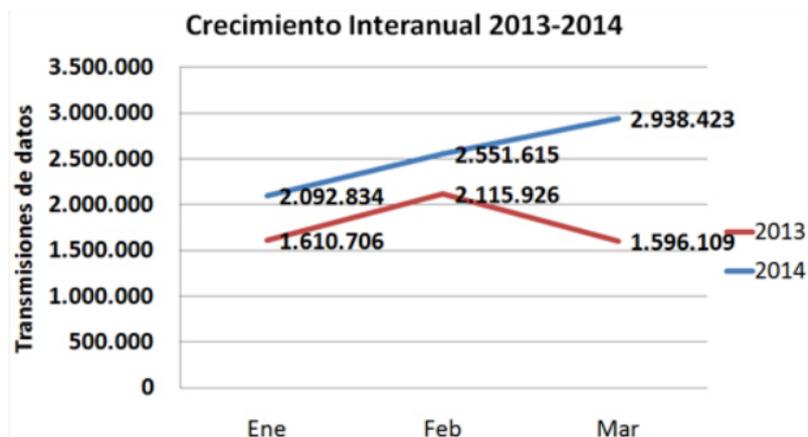
The monitoring of the progress of implementation of the NIF is based on a questionnaire with 52 questions, 3 general and 49 specific, available on the eGovernment portal<sup>iii</sup>. In this regard the participation of Central Government has been intense through its ministerial departments, administrative centers and related entities or subsidiaries, followed by the Autonomous Communities.

As a general conclusion, there is a remarkable adaptation in the following chapters: organizational and technical interoperability, infrastructure and common services, communications and electronic signatures; while, on the contrary, there is a delay in the chapters on semantic interoperability, reuse and, particularly, in the chapter on the electronic document; this chapter is the one with a greater delay and difficulty, among other reasons because it is a subject more novel and requires a multidisciplinary and horizontal treatment within the organization.



**The infrastructure and common services<sup>iv</sup>** enable the progress of interoperability. This is the case especially of the following ones: The Data Intermediation Platform; the Interconnection of Input/Output Registries; the Platform for the validation of electronic signatures @Firma; and Red SARA.

The **Data Intermediation Platform<sup>v</sup>** has grown significantly in the number of data transmissions in the first quarter of 2014, close to 42.36% due to the increase of available services. During the last 2013 this Platform allowed that 30 million documents from citizens were not presented, with an estimated 152 million Euros savings; while the forecast for 2014, with 36 services available will be around 35.5 million data transmissions and will approach 200 Million Euros of savings. It has also been winner of the award to the Public Service of the United Nations within the "Awards Program Public Service United Nations (UNPSA)", in the category of "Improving the delivery of public services"<sup>vi</sup>, the most prestigious international recognition excellence in the public sector.



Regarding the **Interconnection of Input/Output Registries (SIR)**<sup>vii</sup>, during the last May 2014 the system exceeded 300,000 transactions. These transmissions save 3 euros per record, compared to the cost of paper processing, so that only during that month of May, the savings from the transmission were over a million euros. The following public administrations connected to SIR digitized over 95% records as of May 2014:

		Número de registros	% digitalización	Ahorro Costes en euros
<b>COMUNIDAD DE MADRID</b>	LEGANÉS	5678	100%	23053
	MAJADAHONDA	4890	100%	19853
	SAN SEBASTIÁN DE LOS REYES	4354	100%	17677
	GALAPAGAR	2805	100%	11388
	POZUELO DE ALARCÓN	1993	100%	8092
<b>CANARIAS</b>	ARONA	1842	100%	7479
	ARUCAS	243	100%	987
	GARACHICO	206	100%	836
	BUENAVISTA DEL NORTE	166	100%	674
	ANTIGUA	122	100%	495
<b>ASTURIAS</b>	GIJON	1836	98,97%	7377
<b>TOLEDO</b>	CEBOLLA	186	100%	755
<b>SUBDELEGACIONES DEL GOBIERNO</b>	JAÉN	344	97,67%	1364
	SORIA	100	98%	398

The **Platform for the validation of electronic signatures @Firma**<sup>viii</sup> has processed over 100 million transactions in 2013, while the **Red SARA**<sup>ix</sup> interconnects all ministerial departments, autonomous regions, autonomous cities, and more than 3,708 local bodies representing more than 90% of the population.

Moreover, with regard to semantic interoperability, the **Semantic Interoperability Center** (CISE)<sup>x</sup> progresses so that the viewer tool is already available while the editor tool will join soon. The CISE will gradually include data models and encoding tables corresponding to common services, horizontal issues, or of sector interest.

Finally, there is a new online strategy dedicated to '**E-Archiving**'<sup>xi</sup> in the eGovernment portal to serve as a focal point of the question. This line includes sections and links related to the following topics: e-archiving, policy for the management of electronic documents, metadata, electronic document, electronic file, tools for managing electronic documents and records with reference to **INSIDE**<sup>xii</sup>, references to standards and good practices.

Following the wave of March 2014 it is planned to launch a new wave in October to show the progress throughout the year.

This monitoring of the NIF is simultaneous to the one carried out by the European Commission in relation to the alignment with the European Interoperability Framework in theory and in terms of the practical aspects of implementation and monitoring of its evolution.

---

i [https://www.ccn-cert.cni.es/index.php?option=com\\_wrapper&view=wrapper&Itemid=211&lang=es](https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=211&lang=es)

ii [https://www.ccn-cert.cni.es/index.php?option=com\\_wrapper&view=wrapper&Itemid=211&lang=es](https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=211&lang=es)

---

iii

[http://administracionelectronica.gob.es/pae\\_Home/dms/pae\\_Home/documentos/Estrategias/pae\\_Interoperabilidad\\_Inicio/pae\\_Normas\\_tecnicas\\_de\\_interoperabilidad/20140314\\_ENI\\_Cuestionario\\_seguimiento\\_marzo.xlsx](http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad/20140314_ENI_Cuestionario_seguimiento_marzo.xlsx)

iv

[http://administracionelectronica.gob.es/pae\\_Home/pae\\_Estrategias/Racionaliza\\_y\\_Comparte.html#.U5XYqXbwDL8](http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Racionaliza_y_Comparte.html#.U5XYqXbwDL8)

v <http://administracionelectronica.gob.es/ctt/svd>

vi

[http://administracionelectronica.gob.es/pae\\_Home/pae\\_Actualidad/pae\\_Noticias/Anio2014/Mayo/Noticia-CTT-2014-05-28-SVD-UNPSA-2014.html#.U5XV9nbwDL9](http://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2014/Mayo/Noticia-CTT-2014-05-28-SVD-UNPSA-2014.html#.U5XV9nbwDL9)

vii <http://administracionelectronica.gob.es/ctt/sir>

viii <http://administracionelectronica.gob.es/ctt/afirma>

ix <http://administracionelectronica.gob.es/ctt/redsara>

x <http://cise.redsara.es/SGAS/VisorAction.action>

xi

[http://administracionelectronica.gob.es/pae\\_Home/pae\\_Estrategias/Archivo\\_electronico.html#.U5XcInbwDL8](http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico.html#.U5XcInbwDL8)

xii

<http://administracionelectronica.gob.es/ctt/verPestanaGeneral.htm?idIniciativa=inside#.U5Xc13bwDL8>