Translated from Spanish to English - www.onlinedoctranslator.com

centro criptológico nacional

ICT Security Guide

CCN-STIC 803

ENS. Systems assessment

May 2020

MINISTERIO DE DEFENSA

Edit:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.11.17 09:54:50 +01'00'

-National Cryptological Center, 2020

NIPO: 785-17-078-3

Edition Date: May 2020

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained therein, expressly rejecting any type of implied warranty that may be related. In no case can the National Cryptological Center be held responsible for direct, indirect, incidental or extraordinary damage derived from the use of the information and software indicated even when warned of such possibility.

LEGAL WARNING

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

FOREWORD

In an increasingly complex and globalized world, in which information and communication technologies (ICT) play a very important role, we must be aware that the adequate management of cybersecurity constitutes a collective challenge that necessarily we have to face. It is necessary to guarantee the protection of the economic, technological and political capacity of our country, especially when the proliferation of targeted attacks and the theft of sensitive information represent an incontestable reality.

Therefore, it is essential to be up to date on the threats and vulnerabilities associated with the use of new technologies. Knowledge of the risks that loom over cyberspace must serve to safely implement measures, both procedural and technical and organizational, that allow for a safe and reliable environment.

Law 11/2002, of May 6, regulating the National Intelligence Center (CNI), entrusts the National Intelligence Center with the exercise of functions related to the security of information technologies and the protection of classified information, At the same time, it confers on its Secretary of State Director the responsibility of directing the National Cryptological Center (CCN).

Based on the knowledge and experience of the CNI on threats and vulnerabilities in terms of emerging risks, the Center carries out, through the National Cryptological Center, regulated by Royal Decree 421/2004, of March 12, various activities directly related to security. of ICT, aimed at the training of expert personnel, the use of appropriate security technologies and the application of security policies and procedures.

Precisely, this series of CCN-STIC documents is a clear reflection of the work that this organization carries out in terms of security implementation, allowing the application of policies and procedures, since the guides have been prepared with a clear objective: to improve the degree of cybersecurity of organizations, aware of the importance of establishing a reference framework in this matter that serves as support for Administration personnel to carry out the difficult task of providing security to ICT systems under your responsibility.

With this series of documents, the National Cryptological Center, in compliance with its tasks and what is reflected in Royal Decree 3/2010 which regulates the National Scheme in the field of electronic Administration, contributes to improving Spanish cybersecurity and maintain the infrastructures and information systems of all public administrations with optimal levels of security. All of this, in order to generate trust and guarantees in the use of these technologies, protecting the confidentiality of the data and guaranteeing its authenticity, integrity and availability.

May 2020

Paz Esteban Lopez
Secretary of state
Director of the National Cryptological Center

INDEX

1. INTRODUCTION 5
1.1. NEED TO ASSESS..... 5
1.2. ASSESSMENT PROCEDURE 6
1.3. ELECTRONIC NOTIFICATIONS AND PUBLICATIONS..... 7
2. ASSESSMENT CRITERIA 8
2.1. COMMON CRITERIA APPLICABLE TO ALL DIMENSIONS 8
2.2. CRITERIA FOR TYPES OF INFORMATION WITH PERSONAL DATA11
23. CRITERIA FOR THE AVAILABILITY OF SERVICES 13
2.3.1. CRITICAL PERIODS..... 13
2.3.2. RTO (RECOVERY TIME TARGET) 13
2.4. SPECIFIC CRITERIA 14
2.5. SPECIFIC CRITERIA FOR CRITICAL OPERATORS IN THE PUBLIC SECTOR..... 15
3. TYPES OF INFORMATION..... 16
3.1. ID..... 16
3.2. ASSESSMENT..... 17
3.2.1. CONFIDENTIALITY..... 17
3.2.2. INTEGRITY..... 17
3.2.3. TRACEABILITY..... .18
3.2.4. AUTHENTICITY..... 18
4. SERVICES..... 18
4.1. ID..... 18
4.2. ASSESSMENT..... 19
4.2.1. AVAILABILITY..... twenty
5. DETERMINATION OF THE LEVELS AND CATEGORY OF THE SYSTEM 21
5.1. ASSESSMENT OF THE DIMENSIONS OF ESSENTIAL ASSETS..... 21
5.2. DETERMINATION OF SUBSYSTEMS 22
5.3. FORMULATION OF THE CATEGORY OF A SYSTEM..... 22
5.4. THIRD PARTIES..... .2. 3
5.5. DOCUMENTATION..... 24
6. ANNEX A. GLOSSARY OF TERMS 25
7. ANNEX B. ABBREVIATIONS..... 28
8. ANNEX C. REFERENCES 29

1. INTRODUCTION

1. This guide establishes general guidelines that are applicable to entities of different nature, size and sensitivity, without going into particular cases. Each organization is expected to customize them to suit its unique environment.
2. The National Security Scheme establishes a series of security measures in its Annex II that are conditional on the assessment of the level of security in each dimension, and the security category (article 43) of the information system in question. In turn, the security category of the system is calculated based on the highest security level of the valued dimensions.
3. The process for determining levels and categories is established in Annex I, which provides a series of general criteria to determine whether the security requirements are of a HIGH, MEDIUM or LOW level in each of the security dimensions: confidentiality [C], integrity [I], traceability [T], authenticity [A], and availability [D].
4. The National Security Scheme establishes three security categories for information systems: BASIC, MEDIUM and HIGH.
    - An information system will be of HIGH category if any of its security dimensions reaches the HIGH level.
    - An information system will be of MEDIUM category if any of its security dimensions reaches the MEDIUM level and none reaches a higher level.
    - An information system will be of BASIC category if any of its security dimensions reaches the LOW level and none reaches a higher level.
5. This guide aims to define the criteria to determine the level of security required in each dimension and offer recommendations also considering other regulatory frameworks (such as those derived from data protection or the security of critical operators, for example), which may be developed later in their own legislation. To do this, the essential elements, information and services, are analyzed, pivoting around them the criteria that the person responsible for each type of information and each service may use, taking into account that the power to determine the category of the system corresponds to the person responsible for it.

1.1. NEED TO ASSESS

6. Frequently, the value of the system in terms of security is concentrated in a few assets that are the essence and reason for being of the system, called **essential assets**, and in a few**dimensions**. It is advisable to focus on those assets and on those dimensions in which the impact of a

incident may be greater, ignoring those combinations in which the impact is negligible or irrelevant.

7. Having previously identified the services provided by the entity, subject to compliance with the ENS, it is advisable to begin the valuation by type assets**information**used by such services, assessing, in this order: *confidentiality, integrity, traceability, authenticity*and, if relevant, *availability*. It is common that availability is not a relevant attribute of the information and is not assigned to any level.

8. It is advisable to continue with type assets**service**, assessing their availability. The requirements regarding confidentiality, integrity, traceability and authenticity are usually imposed by the types of information handled by each service, assuming those established in the previous paragraph.

9. A system will assume, for each dimension, the maximum value considered for it in the different types of information handled by the services provided.

10. The category of the system is determined by considering the maximum value of all its dimensions, for all the services provided by the system.

1.2. ASSESSMENT PROCEDURE

11. If the entity has created an ICT Committee[1]and a STIC Committee[2], one of the functions of the ICT Committee may be the identification of the types of information that will be managed and the services that will be provided, prioritizing the consideration of the so-called essential assets that may have greater criticality. Once the types of information and services have been defined, one task of the STIC Committee may be to establish the recommended security levels in each dimension for each of these essential assets. These assessments must be approved within the regulatory framework that governs the entity's actions in terms of information security.

12. The levels thus established may be subsequently adjusted by the corresponding managers (Responsible for Information and Services). Ideally, all assessments will be established by regulations.

13. The responsibility for the evaluation of the information and services is exclusively the person responsible for the information and the service, respectively, although it may be proposed by the System Manager, the Security Manager or the STIC Committee and approved. subsequently by the Responsible for the Information or the corresponding Service, if the latter considers it appropriate.

[1]ICT Committee: Information and Communication Technologies.

[2]STIC Committee: Security in Information and Communication Technologies.

14. Except for those issues in which there is a legal or administrative mandate, the opinion of the Security Manager and the System Manager must be collected and considered in the assessment process.

15. Once the assessments of the different types of information that are handled and the different services that are provided have been determined, the Security Manager is responsible for applying the procedure described in Annex I of Royal Decree 3/2010 to, in accordance at the maximum levels of each security dimension and, therefore, of the system category, determine the minimum set of security measures of Annex II of Royal Decree 3/2010 that are applicable in the system, considering the conditions indicated in said Annex.

16. The determination of the category of a system does not imply that, due to this fact, the level of the security dimensions that have not influenced the determination of the system's category is altered. However, it should be taken into account that assigning a category to the system may require raising the maturity level of the measures that are applicable.

17. Finally, the set of measures must be enriched with those that may arise from the regulations relating to personal data, critical infrastructures or any other that establishes requirements on the security of the systems.

1.3. ELECTRONIC NOTIFICATIONS AND PUBLICATIONS

18. The National Security Scheme establishes in its article 32 related to "Technical requirements for electronic notifications and publications" that:

    - *Electronic notifications and publications of resolutions and administrative acts will be carried out in such a way that they comply, in accordance with the provisions of this royal decree, with the following technical requirements:*
        - *Ensure the authenticity of the organization that publishes it.*
        - *Ensure the integrity of the published information.*
        - *Leave a record of the date and time of the resolution or act subject to publication or notification being made available to the interested party, as well as access to its content.*
        - *Ensure the authenticity of the recipient of the publication or notification.*

19. A system that provides an electronic notification or publication service must, first of all, have a security assessment of the information it notifies or advertises. Typically, the assessment of information establishes levels of confidentiality, integrity, traceability and authenticity.

20. The notification or publication service makes these assessments its own, and adds the availability requirements determined by the Service Manager.

21. The category of the system will be expressed based on the maximum levels in each dimension of the types of information managed and the services provided.

2. ASSESSMENT CRITERIA

22. Usually, an individualized assessment of the different types of information and services in the scope of application is carried out, considering the relevant dimensions for each of them.

23. However, the individual assessment of each information handled and each service provided may not be the most effective way of working and may give rise to more heterogeneous scenarios than necessary, both within the same entity and in data exchange systems. information or provision of services. For this reason, it is recommended to first proceed with the assessment of the essential assets that will undoubtedly require the most restrictive assessments in the security dimensions and that will thereby determine the category of the system.

24. This guide includes criteria that may be applicable to one or several dimensions, both types of information and services.

25. Each assessment criterion is coded to facilitate reference when justifying assessment decisions.

2.1. COMMON CRITERIA APPLICABLE TO ALL DIMENSIONS

26. Criteria are established that apply to all dimensions of security (selecting a LOW, MEDIUM or HIGH level, according to the ENS), both types of information and services, considering the consequences of a negative impact on security. of information and services, taking into account, in accordance with article 43 of Royal Decree 3/2010, their impact on the organization's ability to achieve its objectives,
the protection of its assets, the fulfillment of its service obligations, respect for the law and the rights of citizens[3].

27. The impact criteria considered are the following:

- Legal provision: Existence of a legal or administrative provision that conditions the level of the dimension.

[3]In the following tables the expression "N/A" indicates that the dimension is not assigned to any level.

- Direct harm: Existence of direct harm to the citizen, understood as a natural, legal or professional person, and of any nature.

- Failure to comply with a rule: Implies failure to comply with a rule (legal or administrative, regulatory, contractual or internal).
- Economic losses: Implies economic losses for the entity.
- Reputation: Implies reputational damage for the entity.
- Protests: Anticipation that it could lead to protests. Crimes: It would
- facilitate the commission of crimes or hinder their investigation.

COMMON CRITERIA APPLICABLE TO ALL DIMENSIONS OF TYPES OF INFORMATION AND SERVICES					
		Not applicable (N/A)	**LOW**	**HALF**	**HIGH**
Legal provision or administrative		COM.DIS.N There is none legal provision or administrative that conditions your level.	COM.DIS.B By legal provision or administrative: law, decree, order, resolution...	COM.DIS.M By legal provision or administrative: law, decree, order, resolution...	COM.DIS.A By legal provision or administrative: law, decree, order, resolution...
Direct harm to the citizen (of any kind)		COM.PER.N It does not imply any direct harm to the citizen.	COM.PER.B Some damage.	COM.PER.M significant damage, although rectifiable.	COM.PER.A Serious damage, difficult or impossible repair.
Breach of a standard	**Legal or administrative**	COM.LEG.N It does not imply breach of a standard legal.	COM.LEG.B Breach mild formality of a legal norm, of rectifiable character.	COM.LEG.M Breach material of a legal rule, or breach formal not rectifiable.	COM.LEG.A Breach formal and material seriousness of a legal norm.
	Regulatory	COM.REG.N It does not imply breach of regulations of a regulator.	COM.REG.B it implies breach of regulations of a regulator.	COM.REG.M Implies sanction significant of a regulator.	COM.REG.A Implies sanction serious of a regulator and/or loss of license to operate.
	Contractual	COM.CON.N It does not imply breach of an obligation contractual.	COM.CON.B Breach mild formality of an obligation contractual.	COM.CON.M Breach material or formal of an obligation contractual.	COM.CON.A Breach formal or material serious of a obligation contractual.
	Internal	COM.INT.N It does not imply breach of regulations internal.	COM.INT.B Breach mild formality of an internal norm.	COM.INT.M Breach material or formal of a standard internal.	COM.INT.A Breach formal or material serious of an internal norm.

COMMON CRITERIA APPLICABLE TO ALL DIMENSIONS OF TYPES OF INFORMATION AND SERVICES				
	Not Attached (N/A)	**LOW**	**HALF**	**HIGH**
Losses economic	EAT WITH Does not imply losses economic.	COM.ECO.B Economic losses appreciable (not greater than 4% of the annual budget of the organization).	COM.ECO.M Economic losses important (greater than 4% and less than 10% of the annual budget of the organization).	COM.ECO.A Economic losses or alterations financial significant (greater than 10% of the budget annual of the organization).
Reputation	COM.REP.N Does not imply harm reputational.	COM.REP.B reputational damage moderate with citizens or with other organizations.	COM.REP.M reputational damage significant with citizens or with other organizations.	COM.REP.A reputational damage serious with citizens or with other organizations.
protests	COM.PRO.N It is not expected that can flow in protests.	COM.PRO.B Multiple protests individual.	COM.PRO.M Public protests (alteration of order public).	COM.PRO.A Mass protests (serious alteration of public order).
Crimes	COM.DEL.N It would not facilitate commission of crimes nor would it hinder your investigation.	COM.DEL.B I would favor the commission of crimes.	COM.DEL.M would favor significantly the commission of crimes or would hinder their investigation.	COM.DEL.A It could incite the commission of crimes, would constitute a crime in itself, or would make it difficult enormously investigation.

Table 1. Common criteria applicable to all Dimensions of Types of Information and Services

2.2. CRITERIA FOR TYPES OF INFORMATION WITH PERSONAL DATA

28. For the processing of personal data, the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to the processing, will apply. of personal data and the free circulation of these data (RGPD), in addition to the provisions of Organic Law 3/2018, of December 5, on Data Protection and Guarantee of Digital Rights (LOPDGDD) and, especially, the provisions in its first Additional Provision: security measures in the public sector, which prescribes:

"First additional provision. Security measures in the public sector.

1. The National Security Scheme will include the measures that must be implemented in the case of processing of personal data to prevent its loss, alteration or unauthorized access, adapting the criteria for determining the risk in the processing of data to that established in the article. 32 of Regulation (EU) 2016/679.

2. Those responsible listed in article 77.1 of this organic law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of equivalent measures in companies. or foundations linked to them subject to private law.

In cases in which a third party provides a service under a concession, management entrustment or contract, the security measures will correspond to those of the public administration of origin and will comply with the National Security Scheme."

29. The Spanish Data Protection Agency points out in its note "The impact of the general data protection regulation on the activity of public administrations", the following:

    - The *"need to carry out a risk analysis for the rights and freedoms of citizens of all data processing that is carried out. The GDPR makes the application of all the compliance measures it provides for responsible parties dependent on the level and type of risk that each treatment implies for the rights and freedoms of those affected. Therefore, all treatments, both existing and those intended to be initiated, must be subject to a risk analysis. Those responsible and those in charge of processing must carry out a risk analysis for the rights and freedoms of citizens."*

    - *"The determination of compliance measures (including security measures) will depend on the level and type of risk that each treatment implies for the rights and freedoms of those affected."*
    - *"In the case of the AAPP, the application of security measures will be marked by the criteria established in the National Security Scheme."*

30. For all these reasons, the set of measures that ultimately have to be applied, in addition to contemplating the principles of data protection from the design and by default and the rest of the applicable legal precepts, will have to be directed to the protection of the rights fundamentals of the owners of personal data.

31. Finally, remember that, until Directive (EU) 2016/680 of the European Parliament and of the Council, of April 27, 2016, on the protection of natural persons with regard to to the processing of personal data by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, remain in force, exclusively for the processing of this type of data, the
Organic Law 15/1999 and Royal Decree 1720/2007 that develops it, as indicated in the fourth transitional provision of the LOPDGDD.

23. CRITERIA FOR THE AVAILABILITY OF SERVICES

2.3.1. CRITICAL PERIODS

32. Certain services may have a heterogeneous frequency of use, so availability requirements may vary over time. .

33. There are services that are critical only certain days of the month or year. Those responsible must adjust security measures to the criticality at all times. For example, alternative services can be contracted during critical periods, or the service level (SLA) can be raised[4]) required from suppliers.

34. The steps to follow are as follows:

- The Service Manager determines the periods in which each security level is applied (critical periods).
- The Security Manager will adjust the system assessment and determine the necessary measures in each critical period.
- The Security Manager will ensure that the system adjusts at least to the measures determined in each critical period, without prejudice to the security measures being extended beyond the required period for reasons of operational convenience or optimization of resources.

2.3.2. RTO (RECOVERY TIME TARGET)

35. One of the useful criteria for determining the availability requirements of a service is the establishment of a**target recovery time**either**reference interruption time**, which is often known as**RTO**, which indicates the maximum time that the service can remain interrupted.

[4]Service Level Agreement (in Spanish, ANS)

36. Before the maximum time set by the RTO is reached[5] the organization must have achieved the minimum level of service (MBCO[6]) which must have been established by the Service Manager.

37. The availability assessment measures the consequences if this time is exceeded; That is, it remains below the minimum service level for a period greater than the established RTO.

38. Security requirements are sensitive to RTO. A very short RTO (minutes or hours) puts a lot of pressure on the organization to ensure compliance, while a long RTO (days) leaves some room for maneuver.

39. The following tables can be used as a reference.

RTO	< 4 hours	4 hours -1 day	1 day – 5 days	> 5days
level	High	Half	Low	Not applicable

Table 2. Deadlines for determining the availability of services 4h = 4 hours

1d = 1 day = 24 hours

5d = 5 days (1 work week)

CRITERIA FOR THE AVAILABILITY OF SERVICES				
	Not Applicable (N/A)	**LOW**	**HALF**	**HIGH**
RTO – Time Aim of Recovery	DIS.RTO.N The restoration of minimum levels of service can be carried out within a period of more than 5 days (RTO)	DIS.RTO.B The restoration of minimum levels of service must be carried out within a maximum period of 5 days (RTO)	DIS.RTO.M The restoration of minimum levels of service must be done within a maximum period of 1 day (RTO)	DIS.RTO.A The restoration of minimum levels of service must be carried out within a maximum period of 4 hours (RTO)

Table 3. Criteria for determining the availability of services

2.4. SPECIFIC CRITERIA

To facilitate the assessment of different types of organizations, such as Local Entities or Universities, the National Cryptological Center has prepared the Guide CCN-STIC-883 Implementation of the ENS in the EELL.

[5] Recovery Time Objective (in Spanish, TRO).

[6] Minimum level of services and/or products that is acceptable to the organization to achieve its objectives during a disruption

Specifically, Annexes I, II and III of said Guide present the assessment of the security dimensions of asset catalogs (information and services), taking into account the population ranges and the essential role of the Provincial Councils, Island Councils or other organizations. competently responsible for information security and the implementation of Electronic Administration. References to the applicable regulations are included in section 8 of this document.

40. On the other hand, specific criteria for Universities have been included as Annex I of this Guide.

2.5. SPECIFIC CRITERIA FOR CRITICAL PUBLIC SECTOR OPERATORS

41. The types of information identified may contain sensitive information for the security of essential services for society provided by critical operators, including information related to the Operator's Security Plan or the Specific Protection Plans of critical infrastructures.

42. Similarly, the services identified for the different systems can be used for the provision of said essential services.

43. The system categorized with respect to the ENS could be used by a critical infrastructure, contributing to the security guarantee of the provision of an essential service for society.

44. The protection of critical infrastructures has its own legislation (LPIC[7]). In accordance with said regulation, designated critical operators must appoint a Security and Liaison Manager, and for each infrastructure designated as critical, a Security Delegate.

45. When both regulations (ENS, LPIC) are applicable to an entity, the set of applicable security measures must be determined, with the development of a specific CCN-STIC guide contemplated.

46. It will be the Secretary of State for Security through the National Center for the Protection of Critical Infrastructures (CNPIC) that will establish by regulation the criteria to be used for the protection of the essential services of the infrastructures designated as critical in the corresponding sectoral strategic plans.

47. The application of said criteria may require the review of the security measures to be applied or even the adoption of additional measures that may be required by specific legislation or that have been agreed upon by the National Commission for the Protection of Critical Infrastructures. Among other

[7]Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures

measures, may require the legal classification of the information, according to the Official Secrets Law[8] and therefore the necessary accreditation of the classified systems that manage it.

3. TYPES OF INFORMATION

3.1. ID

48. Although *information* is any set of data that has meaning, the National Security Scheme focuses on assessing the services of those entities that, directly or indirectly, are subject to Law 39/2015, of October 1, Common Administrative Procedure of Public Administrations and to Law 40/2015, of October 1, Legal Regime of the Public Sector. Consequently, the types of information to be assessed will be those used by the services within said scope of application.[9]. For example, medical, fiscal, administrative data, contracts, resolutions, notifications, etc. In general, it can be expected that these types of information are identified in some type of general or particular regulation of the entity, which gives them their own entity and implies duties of the public sector regarding the processing of said type of information.

49. Auxiliary data that are not the direct object of the administrative process or are not included in the powers of the entity in question, and only appear as instrumental for the provision of services, will not be directly assessed. For example, directory services, access keys, etc.

50. For each type of information, it must be determined:

- Her name, which uniquely identifies her.
- Your manager, who establishes your security requirements.
- Other characteristics that are considered relevant for operational, vulnerability association, risk estimation or audit purposes.

51. The determination of the types of information and the figure of its Controller or Controllers will be determined in the Security Policy or, failing that, the Security Policy will establish the framework for its identification and the procedure for designating the person(s). responsible persons).

[8] Law 9/1998, of April 5, on official secrets.

[9] For more details, see CCN-STIC Guide 830 Scope of application of the ENS.

3.2. ASSESSMENT

52. The assessment of the information is determined by the person responsible for it, taking into account its nature and the regulations that may apply to it. This assessment requires legal knowledge of the matter in question.

53. Information often imposes relevant requirements on the dimensions of **confidentiality**,**integrity**,**traceability**and**authenticity**. There are usually no relevant requirements in the dimension of**availability**, which is considered in the services that manage that information.

54. When a dimension does not condition security measures, in the assessment section it will be indicated as "**Not applicable**" either "**N/A**".

55. Criteria for establishing a value in each dimension are described below. These criteria are of a general and indicative nature, and the security policy may specify particular cases of the entity and the person responsible for the information may justify the assignment that he determines is appropriate.

3.2.1. CONFIDENTIALITY

56. The General Criteria of section 2.1 are applicable, considering the consequences that its**disclosure to unauthorized persons or persons who do not need to know the information**.

57. The Criteria for Personal Data, detailed in section 2.2, apply.

58. The specific Criteria determined for specific areas that may be published as annexes to this guide or by the organization's security policy will apply, in accordance with section 2.5.

- The assessment of the dimension will not be applicable (N/A) when it involves information of a public nature, accessible by anyone.

3.2.2. INTEGRITY

59. The General Criteria of section 2.1 are applicable, considering the consequences that its**modification by someone who is not authorized to modify the information.**

60. The Criteria for Personal Data, detailed in section 2, apply.

61. The specific Criteria determined for specific areas that may be published as annexes to this guide or by the organization's security policy will apply, in accordance with section 2.5.

62. The assessment will not be applicable (N/A) to the dimension:

- when errors in its content have no consequences. when errors
- in its content are easily and quickly repairable.

3.2.3. TRACEABILITY

63. The General Criteria of section 2.1 are applicable, considering the consequences that the**not being able to check a posteriori who has accessed, or modified, certain information**.

64. The Criteria for Personal Data, detailed in section 2.2, apply.

65. The specific criteria determined for specific areas that may be published as annexes to this guide or by the organization's security policy will apply, in accordance with section 2.5.

66. The assessment will not be applicable (N/A) to the dimension:

- when major errors cannot occur, or are easily repairable by other means.
- when relevant crimes cannot be perpetrated, or their investigation is easily achievable by other means.

3.2.4. AUTHENTICITY

67. The General Criteria of section 2.1 are applicable, considering the consequences that would have**the fact that the information was not authentic**.

68. The Criteria for Personal Data, detailed in section 2, apply.

69. The specific Criteria determined for specific areas that may be published as annexes to this guide or by the organization's security policy will apply, in accordance with section 2.5.

70. The assessment will not be applicable (N/A) to the dimension:

- when the origin is irrelevant or widely known by other means.
- when the recipient is irrelevant, for example, because it is anonymously disseminated information.

4. SERVICES

4.1. ID

71. For the purposes of this guide,*service*that provided by the information systems of the entity that is subject, directly or indirectly, to Law 39/2015, of October 1, Common Administrative Procedure of Public Administrations and Law 40/2015, of October 1, Legal Regime of the Public Sector.

72. Some of these services may be identified in some type of general order, while others will be specific to the entity. In any case, the services contemplated here have their own identity regardless of the means used to provide them, with the entity that provides them assuming obligations with respect to them.

73. Internal, auxiliary or instrumental services such as email, network files, directory services, printing, backup copies, etc. are not valued, unless they constitute essential elements for the provision of services to citizens.

74. For each service, the following must be determined:

- Your name, which uniquely identifies you.
- Your manager, who establishes your security requirements.
- Other characteristics that are considered relevant for operational, vulnerability association, risk estimation or audit purposes.

75. The determination of the services provided and the figure of the person responsible will be determined in the Security Policy or, failing that, the Security Policy will establish the framework for its identification and the procedure for designating the person responsible.

4.2. ASSESSMENT

76. The assessment of a service is determined by the person responsible for it, taking into account the nature of the service and the regulations that may apply to it. This assessment requires legal knowledge of the matter in question.

77. Services typically establish relevant requirements in terms of **availability**. It is also common for the other security requirements on the services to derive from those of the information that is used.

78. The level of security required in terms of availability will be established based on the consequences of an authorized person not being able to use the service when needed.

79. The requirements of**confidentiality**,**integrity**,**traceability**and **authenticity** about a service derive from the information it handles. Incidents in the authentication or authorization of the service may imply incidents of confidentiality of the managed information. In the case of integrity, it includes the possibility that information may be incomplete or inaccurate because the service is not completed properly. An error in authentication can lead to inauthentic information or incorrect traceability of changes to it.

80. When a dimension does not condition security measures, in the evaluation section it will be indicated as**"Not applicable**" either**"N/A."**

81. Below are criteria to establish a value in the relevant dimension in a service: availability. These criteria are of a general and indicative nature, and the security policy may specify particular cases of the entity, and the person responsible for the information may justify the assignment that he or she determines is appropriate.

4.2.1. AVAILABILITY

82. The General Criteria of section 2.1 are applicable, considering the consequences that would have**that an authorized person or interconnected system could not use the service when needed within the service period established and announced by the organization.**

83. The Criteria for Availability, detailed in the section 23.

84. The specific criteria determined for specific areas that may be published as annexes to this guide or by the organization's security policy will apply, in accordance with section 2.4.

85. The assessment will not be applicable (N/A) to the dimension when the restoration of minimum service levels in a period of more than 5 days (RTO) has hardly any adverse consequences.

5. DETERMINATION OF THE LEVELS AND CATEGORY OF THE SYSTEM

5.1. ASSESSMENT OF THE DIMENSIONS OF ESSENTIAL ASSETS

86. For each essential asset, whether information type or service type, an assessment of its level (low, medium or high) in each security dimension is requested (see Annex I of the ENS):

-For Services: Availability (D).

-For Types of Information: C (Confidentiality), I (Integrity), T (Traceability) and A (Authenticity).

87. When a system handles different types of information and provides different services, the level of the system in each dimension will be the highest of those established for each type of information and each service.

Asset name essential	guy[10]	Celeven	Yo	T	TO	d
Maximum value of the level recorded in safety dimensions						

Figure 1. Categorization of a System based on the Levels in each Dimension of its Essential Assets.

88. The category, in terms of security, modulates the balance between the importance of the information it handles, the services it provides and the security effort required, depending on the risks to which it is exposed, under the criterion of the principle of proportionality.

89. The security levels determined for the information will be attributed to all assets that handle the corresponding information. The security levels determined for the services will be attributed to all assets that are used to provide the corresponding service.

[10]Type: Information or Service.

[eleven]C (Confidentiality), I (Integrity), T (Traceability), A (Authenticity) and D (Availability). For each security dimension, the levels Low, Medium, High or N/A (Not assigned to any level) will be chosen.

5.2. DETERMINATION OF SUBSYSTEMS

90. It may happen that different assets of the same system are subject to different requirements, due to the fact that they serve different types of information or services. This will lead to fragmenting an information system into several subsystems or assuming for the entire set the highest level to which its security dimensions are subject.

91. It is advisable that the set of security measures adopted be as homogeneous as possible, with the smallest number of unique assets to which different measures should be applied. The main reason for not having a homogeneous criterion is usually economic, when some protection measures are high cost and must be applied to the smallest number of assets possible. As examples of measures that should be limited, we can mention encryption equipment, alternative equipment if high availability is required, etc.

92. The category of each subsystem is determined based on what is established in Annex I of RD 3/2010.

93. The applicability of the measures described in Annex II of RD 3/2010 will be determined for each subsystem.

94. An information system complies with RD 3/2010 when all its subsystems comply, according to the security levels for each dimension and the category that corresponds in each case.

95. The category of the system (basic, medium or high) will be determined from the dimensions in accordance with the previous section, or, when subsystems have been defined, from the highest category of the subsystems that make up it in the case that decide to consider them in a single system.

Subsystems	Category[12]
Subsystem 1...	
Subsystem 2...	
Maximum value of the subsystem category	

Figure 2. Categorization of a System based on its Subsystems.

5.3. FORMULATION OF THE CATEGORY OF A SYSTEM

96. The way to represent the category of a system will be as follows, explaining the level in each dimension to help determine the exact security measures that have been applied:

[12]It can be BASIC, MEDIUM or HIGH.

CATEGORY (BASIC-MEDIUM-HIGH): [C=(N/ABMA), I= (N/ABMA), D=(N/ABMA), A=(N/ABMA), T= (N/ABMA)]

97. Below are the security dimensions that have been assigned:

Category that has been assigned to the system(s) of << Entity Name>> is:
(Category): [C(Level), I(Level), T(Level), A(Level), D(Level)]

Figure 3. Categorization of a System along with the Levels in its Dimensions Security.

Examples:

BASIC CATEGORY: [C(N/A), I(B), T(B), A(B), D(B)]

MIDDLE CATEGORY: [C(N/A), I(B), T(B), A(M), D(B)]

HIGH CATEGORY: [C(M), I(B), T(B), A(M), D(A)]

5.4. THIRD PARTIES

98. In general, the security requirements of other systems that depend on the services provided by the analyzed system will be requirements of the analyzed system.

99. When a system uses third-party systems to manage information or to provide services, its own valuation (the level determined for each dimension) of those essential assets will be imposed as a minimum acceptable to the collaborating third party. This assessment will be formally communicated to the System Manager and the Security Manager so that it adjusts to the level in each dimension and, with this, the set of minimum security measures required or required can be determined.

- The requirements of this system become the requirements of the systems used.

100. When a system handles information from third parties or provides services to third parties, its own assessment (the level in each dimension) of the types of information and services will be at least that determined by said third party.

- The requirements of other systems that depend on the services provided by this system are requirements of this system.

101. When a system handles personal data transferred by others or transfers personal data to others, those required by the personal data processing regulations will be added to the security measures required by the National Security Scheme.

102. When a system contributes to the provision of essential third-party services or contains information that may put the security of those essential third-party services at risk, it must be determined whether additional measures should be added to the security measures required by the National Security Scheme. required by critical infrastructures.

5.5. DOCUMENTATION

103. It is essential that all activities related to the evaluation of the systems are perfectly documented:

- criteria followed and reasoning applied, for which the coding of the assessment criteria provided in this guide can be used.
- opinions or considerations of third parties that have been considered
- relevant. applicable laws, regulations, standards or sectoral practices.
- particular circumstances that may have an impact on the valuation, permanently or temporarily, including:
    - critical periods of service provision,
    - aggregation of information or services,
    - special benefit circumstances such as emergency situations
    - third party reviews, including audit.

104. All decisions must be duly and formally approved, as well as the documentation available, for audit purposes.

- The person responsible for each Information approves the assessment of said information.
- The person responsible for each Service approves the assessment of said service.
- The Security Manager determines and approves the security measures that are applicable (**Statement of Applicability**) in the system or in each subsystem and the organizational and technical actions that are adopted to substantiate said security measures.
- If decisions are made to partially or totally suspend a system, these will be approved by the System Manager and those responsible for the Services affected by the suspension.
- The Information and Service Managers must also approve the residual risk entailed by the adoption of the corresponding security measures.
- Finally, these systems will be subject to an audit in accordance with the provisions of art. 34 and Annex III of the ENS.

6. ANNEX A. GLOSSARY OF TERMS

Risk assessment

Global process comprising risk identification, risk analysis and risk assessment (ISO Guide 73:2009).

Authenticity

Property or characteristic that an entity is who it says it is or that it guarantees the source from which the data comes. ENS.

STIC Committee

Commission that brings together those responsible for ICT security and makes coordination decisions. CCN-STIC 402 Guide.

Confidentiality

Property or characteristic that the information is neither made available nor revealed to unauthorized individuals, entities or processes. ENS.

Personal data

Any information about an identified or identifiable natural person ("the interested party"); An identifiable natural person is any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements specific to identity. physical, physiological, genetic, mental, economic, cultural or social of said person. Regulation (EU) 2016/679 (GDPR).

Information

Specific case of a certain type of information. **Information.**

An instance of an information type. FIPS 199.

Integrity

Property or characteristic that the information asset has not been altered in an unauthorized manner. ENS.

Security policy

Set of guidelines expressed in a written document, which govern the way in which an organization manages and protects the information and services it considers critical. ENS.

Information Manager

Person who has the power to establish the requirements for security information.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. CNSS Inst. 4009.

Security Manager

Person who has the power to determine decisions to satisfy the security requirements of information and services.

The**Computer Security Program Manager**(and support staff) directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization. NIST Special Publication 800-12.

Information systems security manager (ISSM). Individual responsible for a program, organization, system, or enclave's information assurance program. CNSS Inst. 4009.

Responsable of the service

Person who has the power to establish the requirements of a service in terms of security.

System Manager

Person in charge of operating the information system.

Information System Owner (or Program Manager). Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. CNSS Inst. 4009, Adapted.

Service

Function or benefit performed by some official entity intended to take care of the interests or satisfy the needs of citizens.

Information system

Organized set of resources so that information can be collected, stored, processed or treated, maintained, used, shared, distributed, made available, presented or transmitted. ENS.

Information System.A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. 44 USC, Sec. 3502; OMB Circular A-130, Appendix III.

Type of information

A specific category of information (for example, personal data, medical data, financial data, investigations, contracts, sensitive information, ...). These types are defined by an organization and, in some cases, are defined by some legal regulations.

Information type. A specific category of information (eg, privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. FIPS 199.

Traceability

Property or characteristic consisting of which the actions of an entity can be attributed exclusively to said entity. ENS.

7. ANNEX B. ABBREVIATIONS

Acronym	Definition
ANS	Service Level Agreement (SLA)
ENS	National Security Scheme
LOPDGDD	Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of the digital rights
LPIC	Law 8/2011, of April 28, which establishes measures for the protection of critical infrastructures.
MAGERIT	Risk Analysis and Management Methodology Information Systems
MBCO	Minimum level of services and/or products that is acceptable for the organization to achieve your goals during a disruption.
GDPR	Regulation (EU) 2016/679.
RTO	Recovery Time Objective (TRO)
SLA	Service Level Agreement (in Spanish, ANS)
TRO	Recovery Time Objective (RTO)

8. ANNEX C. REFERENCES

• 2001/264/EC Council Decision of March 19, 2001 by which adopt the Council's safety standards.

• Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and the free circulation of these data

• Law 9/1998, of April 5, on official secrets

• Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights

• Royal Decree 3/2010 of January 8, which regulates the National Security Scheme in the field of Electronic Administration

• Royal Decree 4/2010, of January 8, which regulates the National Interoperability Scheme in the field of Electronic Administration

• Royal Decree 951/2015, of October 23, modifying Royal Decree 3/2010, of January 8, which regulates the National Security Scheme in the field of Electronic Administration

• Royal Decree 421/2004, of March 12, which regulates the National Cryptological Center

• Technical security instruction in accordance with the National Security Scheme by Resolution of October 13, 2016, of the Secretary of State for Public Administrations

• Technical Security Instruction of the State of Security Report by Resolution of October 7, 2016, of the Secretary of State for Public Administrations

• ICT security guide - (CCN-STIC-801) - National Security Scheme: Roles and Functions. February 2011.

• ICT security guide - (CCN-STIC-830) - Scope of application of the National Security Scheme

• ICT security guide – (CCN-STIC-883) - Implementation of the ENS for EELL

The Annexes to Guide 883 present Specific Compliance Profiles and examples of Adequacy Plans for EELL based on population ranges.

- Small town councils with limited resources, with less than 5,000 inhabitants:
  - either Annex I. Adaptation Plan for Town Councils with less than 20,000 inhabitants.
  - either CCN-STIC 883A - Specific Compliance Profile Small town councils with limited resources (<5,000 inhabitants).

• Town councils between 5,000 and 20,000 inhabitants: either

Annex I. Adaptation Plan for Town Councils with less than 20,000 inhabitants.

either CCN-STIC 883B - Specific Compliance Profile for Town Councils with less than 20,000 inhabitants.

• Town councils between 20,000 and 75,000 inhabitants: either

Annex II. Adaptation Plan for Town Councils between 20,000 and 75,000 inhabitants.

either CCN-STIC 883C - Specific Compliance Profile Town councils between 20,000 and 75,000 inhabitants.

• Provincial Councils, Town Councils, Island Councils or Equivalent Competent Body: either

Annex III. Adaptation Plan for Provincial Councils, Town Councils, Island Councils or equivalent competent body.

either CCN-STIC 883D - Specific Compliance Profile Provincial Councils.

• MAGERIT – version 3. Risk Analysis and Management Methodology Information systems. Higher Council of Electronic Administration, 2012.

• FIPS 199 Standards for Security Categorization of Federal Information and Information Systems. Feb. 2004.

• SP 800-60 Rev.1 Guide for Mapping Types of Information and Information Systems to Security Categories. Volume 1: Guide. Volume 2: Appendices. Aug 2008.