CCN-CERT

# BP/14

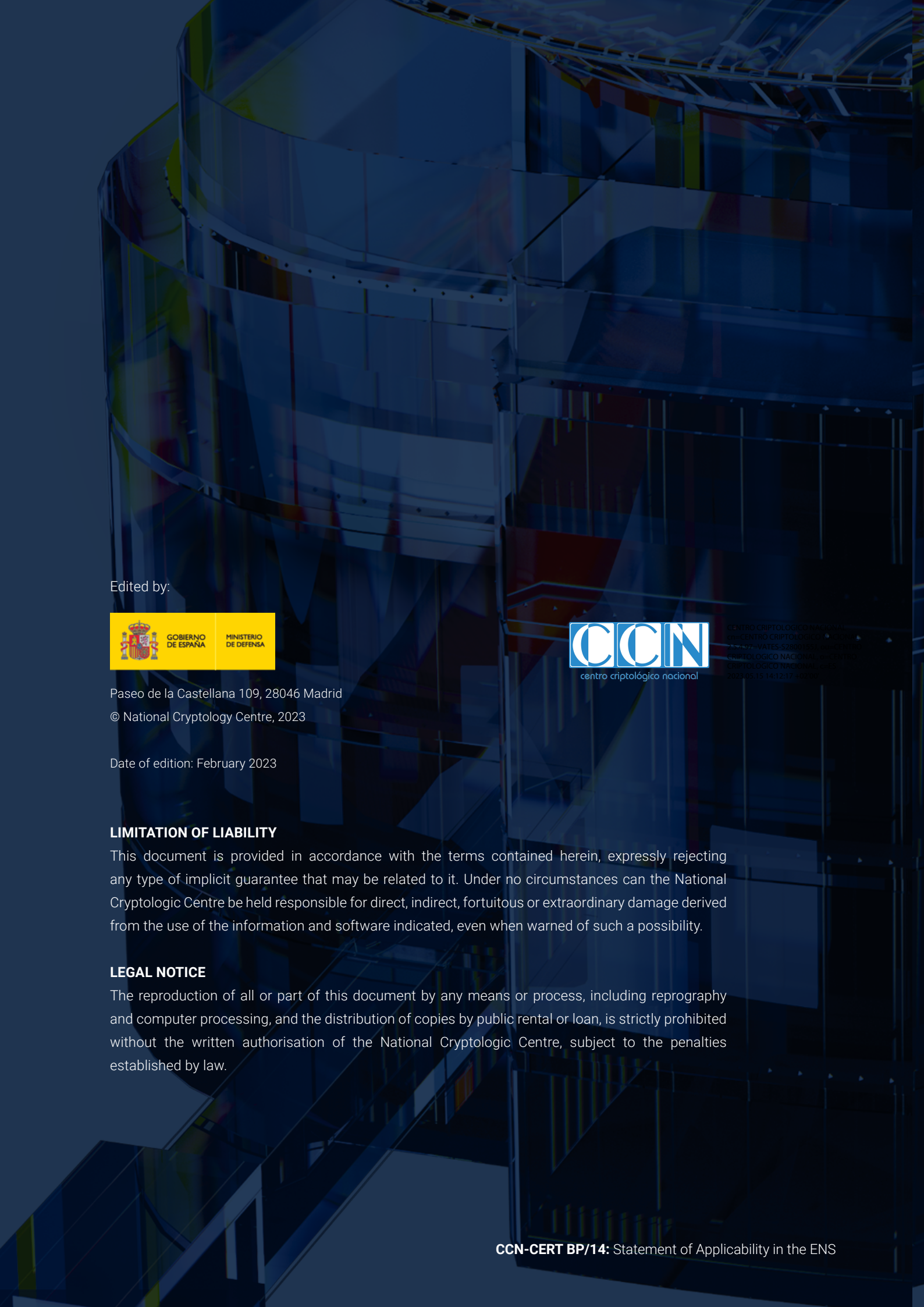

# Statement of Applicability in the ENS

BEST PRACTICE REPORT

FEBRUARY **2023**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Edited by:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Paseo de la Castellana 109, 28046 Madrid


Date of edition: February 2023

# Index

# 1. About CCN-CERT, National Governmental Cert

The CCN-CERT is the Information Security Incident Response Capacity of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by the RD 311/2022 of 3 May.

**The CCN-CERT is the Information Security Incident Response Capacity of the National Cryptologic Centre**

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively face cyber-threats, including the coordination at state public level of the different existing Incident Response Capabilities or Cybersecurity Operations Centres.

All of this, with the ultimate aim of achieving a safer and more reliable cyberspace, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Public Sector Legal Set of rules, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incident management will be carried out by the CCN-CERT in coordination with the CNPIC.

# 2. Introduction

The Statement of Applicability, within the scope of the ENS, is the document that formalises the list of security measures applicable to the information system in question, according to its category, and which are included in Annex II of Royal Decree 311/2022, of 3 May, which regulates it.

As determined in Article 38.3 of the ENS, the security measures referenced in Annex II may be replaced by other compensatory measures provided that it is documented that they provide equal or better protection against the risk to the assets and that the basic principles and minimum requirements set out in Chapters II and III of Royal Decree 311/2022 are met.

Likewise, as indicated in the CCN-STIC-808 guide Verification of compliance with the measures in the ENS, some complementary surveillance measures may be implemented to supplement and balance the requirements that have been implemented for a given security measure, whether basic or reinforcement, when these are not sufficient, in the organisation's opinion, to achieve compliance with the ENS for that measure. They may also complement a compensatory measure that fails to match or improve the risk of the original measure. Sometimes such measures will be transitional (time-limited) until full effectiveness is achieved in the implementation of a measure.

**The Statement of Applicability, within the scope of the ENS, is the document that formalises the list of security measures applicable to the information system in question, according to its category**

As an integral part of the Declaration of Applicability, the correspondence between the compensatory measures implemented and the compensating measures in Annex II shall be detailed, as well as any additional measures that may be required, and shall be formally approved by the Security Officer.

The formalised Statement of Applicability document will be essential for the preparation of the adequacy plan and the subsequent implementation of the measures contemplated, and may be analysed by the certification body and used as a support document during the audit process for the validation of compliance with the ENS. To this end, it is important that the Statement of Applicability indicates for each of the 73 security measures included in the ENS, not only whether it applies to the information system or to the organisation, but also, in a very summarised form, how it applies and/or the documentation where it is detailed and, if applicable, why it does not apply.

**The formalised Statement of Applicability document will be essential for the preparation of the adequacy plan and the subsequent implementation of the measures contemplated**

# 3. Procedure for defining the Declaration of Applicability

In order to bring an information system into compliance with the provisions of the ENS and to be able to determine which measures apply, it is necessary to categorise it and to follow the indications specified in Annex I of the ENS.

The purpose of the categorisation process is to assign a BASIC, MEDIUM or HIGH category to information systems. The security category of an information system seeks to strike a balance between the importance of the information it handles, the services it provides and the security effort required, and the risks to which it is exposed, under the criteria of the principle of proportionality.

In other words, the security measures to be applied to the information system, and so stated in the Statement of Applicability, will come primarily from the categorisation of the system as a result of a set of assessed measures (baseline requirements and mandatory reinforcements), but may sometimes also be eligible as a result of risk mitigation actions that have been assessed as unacceptable (optional reinforcements or mandatory reinforcements for a higher category).

The category is determined on the basis of the assessment of the impact that an incident affecting the security of information or services would have on the dimensions of security: **availability [D], authenticity [A], integrity [I], confidentiality [C]** or **traceability [T]**, following the procedure established in Annex I of Royal Decree 311/2022.

**The purpose of the categorisation process is to assign a BASIC, MEDIUM or HIGH category to information systems**

# 3.1. Categorisation

The determination of the **category of a system** (BASIC, MEDIUM or HIGH) is based on the assessment of the impact on the organisation of an incident affecting the security of that information system, with an impact on the organisational ability to:

**a. Achieve its objectives.**
**b. Protect the assets in its care, including information.**
**c. Fulfil their daily duty obligations.**
**d. To respect the law in force.**
**e. Respect the rights of individuals.**

In addition to each security dimension, the assessment of this impact is carried out individually for each asset of the information system, which is why it is necessary to have an updated inventory of these assets.

It is recommended, in the first place, to assess the essential assets (information and services), which are those that will require the most exhaustive assessment when establishing security levels according to the dimensions, and which will thus determine the system's category. The essential assets are those that concentrate the value of the system in terms of security and are the essence and raison d'être of the system. The rest of the assets will support these essential assets, inheriting their valuations based on their dependency relationship.

Depending on whether the asset is a service to be provided, or information handled by them, it is advisable to focus on the assessment of specific security dimensions. For example, it is recommended to assess the **confidentiality** and **integrity** dimensions **(C, I)** for information type assets, while the **availability** dimension **(D)** is usually associated with service type assets.

The other two (2) dimensions, such as **authenticity (A)** and **traceability (T)**, will be associated indistinctly with services or information, depending on what best suits the organisation; the important thing is that, in one way or another, they are considered if applicable.

**The determination of the category of a system is based on the assessment of the impact on the organisation of an incident affecting the security of that information system**

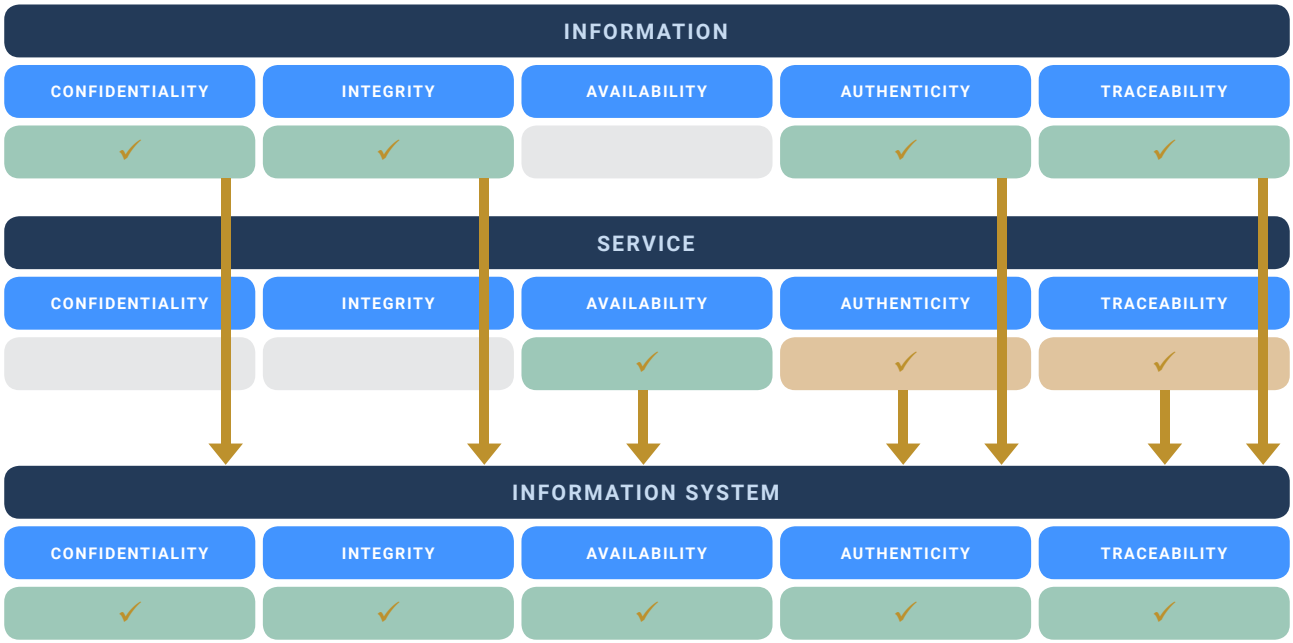



Illustration 1. Assessment of security dimensions according to the type of asset

### 3.1.1 Determination of Security Levels per Dimension

The National Security Framework establishes three (3) security levels to be assigned to the different dimensions: **Low [L], Medium [M]** and **High [H]**.

The determination of the security level (in each dimension) will be obtained on the basis of the assessment of the impact on the institution of the materialisation of the following risks:

- **Legal provision**: existence of a legal or administrative provision that conditions the level of the dimension.
- **Direct harm:** existence of direct damage to the citizen.
- **Non-compliance with a rule:** implies non-compliance with a rule (legal, regulatory, contractual or internal).
- **Economic losses:** implies economic losses for the entity.
- **Reputation:** implies reputational damage for the entity.
- **Protests:** anticipation that it may lead to protests.
- **Crime:** would facilitate the commission of crime or make it more difficult to investigate.

**TABLE 1. COMMON CRITERIA APPLICABLE TO ALL DIMENSIONS OF TYPES OF INFORMATION AND SERVICES**

| | | UNATTACHED | UNDER | MEDIUM | HIGH |
|---|---|---|---|---|---|
| **Legal or administrative provision** | | There is no legal provision conditioning their level. | By legal or administrative provision: law, decree, order, regulation... | By legal or administrative provision: law, decree, order, regulation... | By legal or administrative provision: law, decree, order, regulation... |
| **Direct harm to the citizen** | | No direct harm to the citizen | Some harm to the citizen | Significant, but remediable damage to the citizen | Serious damage, difficult or impossible to repair for the citizen. |
| **Non-compliance with a Standard** | **Legal** | Does not imply non-compliance with a legal rule | Minor formal non-compliance with a legal rule, which can be remedied | Material breach of a legal rule, or a formal breach that cannot be remedied | Serious breach of a legal rule |
| | **Regulatory** | Does not imply non-compliance with the rules of a regulator | Implies non-compliance with the rules of a regulator | Involves significant sanctioning of a regulator | Implies severe sanction by a regulator and/or loss of licence to operate |
| | **Contractual** | It does not imply a breach of a contractual obligation | Minor breach of a contractual obligation | Material or formal breach of a contractual obligation | Serious breach of a contractual obligation |
| | **Internal** | Does not imply non-compliance with internal regulations | Minor breach of an internal rule | Material or formal non-compliance with an internal rule | Serious breach of an∑internal rule |
| **Economic losses** | | No financial loss | Significant financial loss (less than 4% of the organisation's annual budget) | Significant financial losses (equal to or more than 4% and less than 10% of the organisation's annual budget) | Significant economic loss or financial disruption (equal to or greater than 10% of the organisation's annual budget) |
| **Reputation** | | No reputational damage | Appreciable reputational damage with citizens or other organisations | Significant reputational damage with citizens or other organisations | Serious reputational damage with citizens or other organisations |
| **Protests** | | It is not expected to lead to protests. | Multiple individual protests. | Public protests (disturbance of public order) | Mass protests (serious disturbance of public order) |
| **Offences** | | It would not facilitate the commission of crimes or hinder their investigation. | It would encourage the commission of crimes | It would significantly facilitate the commission of crimes or make their investigation more difficult. | It would incite the commission of offences, constitute an offence in itself, or make it very difficult to investigate. |

### 3.1.2 Determination of Category

The National Security Framework establishes three (3) **security categories** for information systems: BASIC, MEDIUM and HIGH:

- An information system shall be of **HIGH category** if any of its security dimensions reaches the High Level.
- An information system shall be of **MEDIUM category** if any of its security dimensions reaches the Medium level and none reaches a higher level.
- An information system shall be of **BASIC category** if any of its security dimensions reaches the Low level and none reaches a higher level.

The determination of the category of a system does not imply that the level of safety dimensions that have not influenced the determination of the system's category is thereby altered. However, it should be borne in mind that assigning a category to the system requires setting the maturity level of the measures to be applied.

**The determination of the category of a system does not imply that the level of safety dimensions that have not influenced the determination of the system's category is thereby altered**

# 3.2. Determination of implementing measures

In order to achieve compliance with the basic principles and minimum requirements set out in the National Security Framework, a set of security measures must be applied, which will be proportionate to the relevant security dimensions of the system to be protected and its category.

Annex II of Royal Decree 311/2022 sets out the correspondence between the security levels required in each dimension and the applicable security measures.

Specifically, for each security measure, the following is indicated:

- Whether its application is determined on the basis of the category of the system or on the basis of the security level assigned to one or more security dimensions.
- Whether or not it is applicable for a given security level. In case the application of the measure is not necessary to obtain the adequacy with the ENS, the value **"n.a."** is given in the table of Annex II.

On the other hand, if its application is necessary, one of the following values will appear:

- **"applies":** indicates that the **basic requirements** of a security measure must be applied to one or more dimensions of security at some level.
- **"+Rn":** where 'n' can take values from '1' to '9', it indicates that such **mandatory reinforcement** must be applied to one or more security dimensions at some level.

Several mandatory reinforcements may apply simultaneously to one or more dimensions of security at some level, e.g. 'R1 + R2 + R5'. Similarly, it may be required to choose a particular mandatory reinforcement from a subset of them, e.g. 'R1 or R2 or R3'. Both cases may be combined, e.g. '[R1 or R2 or R3] + R9'.

**A set of security measures must be applied, which will be proportionate to the relevant security dimensions of the system to be protected and its category**

The following are some examples of the above:

**a** • The measure [org.1] applies to systems of any category. The level of requirement of the measure does not vary according to the category associated with the system; only the **baseline requirements** apply to any category.

| Affected | BASIC | MEDIUM | HIGH | Security measure | |
|---|---|---|---|---|---|
| Category | applies | applies | applies | [org.1] | Security policy |

**b** • The measure [mp.if.6] applies to systems whose security level associated with the *availability* dimension is Medium or High. The level of requirement of the measure does not vary depending on whether the level is Medium or High; in either case only the **baseline requirements** apply.

| Affected | LOW | MEDIUM | HIGH | Security measure | |
|---|---|---|---|---|---|
| D | n.a. | applies | applies | [mp.if.6] | Flood protection |

**c** • The measure [mp.si.2] applies to systems whose security level associated with the *confidentiality* or integrity dimensions is Medium or High. The level of requirement of the measure changes if either of the levels is Medium or High. The **base requirements** are the same for Medium and High Level, while the optional reinforcements only apply for High Level in these two (2) dimensions.

| Affected | LOW | MEDIUM | HIGH | Security measure | |
|---|---|---|---|---|---|
| C I | n.a. | applies | +R1 +R2 | [mp.si.2] | Cryptography |

**c** • Measure [mp.com.4] does not apply to BASIC category, the level of requirement of the measure being different depending on whether the category is MEDIUM or HIGH. The **basic requirements** apply to both categories; for MEDIUM category a choice shall be made between applying the **mandatory reinforcement** R1, R2 or R3; while for HIGH category the **mandatory reinforcement** R4 shall always apply, together with whichever of R2 or R3 is considered to be chosen.

| Affected | BASIC | MEDIUM | HIGH | Security measure | |
|---|---|---|---|---|---|
| Category | n.a. | + [R1 o R2 o R3] | + [R2 o R3] + R4 | [mp.com.4] | Separation of networked information flows |

# 4. Example

## 4.1. Categorisation

Let us assume a simple example of a Local Entity that, due to its public nature, falls under the scope of the ENS.

We follow the next steps:

1 · **Inventory of assets**
Instead of conducting the complete inventory, we focus on those assets that are essential for the Information System in the defined scope:

- Information associated with the Municipal Register of Inhabitants (PMH).
- Information associated with the Register.
- Municipal Register of Inhabitants Service (PMH).
- Registration Service.

2 · **Asset valuation**
After analysing the impact that an incident could have on critical assets, the security levels assigned, by dimension, are as follows:

| INFORMATION ASSETS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| PMH Information | n.a. | [M] | [M] | [M] | [M] |
| Register Información | n.a. | [M] | [M] | [M] | [M] |

| SERVICE ASSETS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| PMH Service | [M] | n.a. | n.a. | [B] | [B] |
| Register Service E/S | [M] | n.a. | n.a. | [B] | [B] |

The security levels of integrity and *confidentiality* have not been assessed for "Service" type assets (value set to **"n.a."**) as it has been considered that they inherit from those assigned to "Information" type assets. Similarly, for "Information" type assets, the security level associated with availability has been determined by the level associated with services.

### 3 · Value bundling and inheritance

| INFORMATION ASSETS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| PMH Information | [M] | [M] | [M] | [M] | [M] |
| Register Information | [M] | [M] | [M] | [M] | [M] |
| Maximum level of the info | [M] | [M] | [M] | [M] | [M] |

| SERVICE ASSETS | [D] | [I] | [C] | [A] | [T] |
|---|---|---|---|---|---|
| PMH service | [M] | [M] | [M] | [B] | [B] |
| Register service E/S | [M] | [M] | [M] | [B] | [B] |
| Maximum level of the services | [M] | [M] | [M] | [B] | [B] |

| MAXIMUM VALUES OF THE SYSTEM | [D] | [I] | [C] | [A] | [T] | MAXIMUM VALUE |
|---|---|---|---|---|---|---|
| PMH Information | [M] | [M] | [M] | [M] | [M] | [M] |
| Register Information | [M] | [M] | [M] | [M] | [M] | [M] |

The system levels shall be: [D] = M, [I] = M, [C] = M, [A] = M and [T] = M.

### 4 · Determination of category

**The category of the information system is determined by the highest security level assigned to some dimension, for some specific asset.**

| MAXIMUM VALUES OF THE SYSTEM | [D] | [I] | [C] | [A] | [T] | MAXIMUM VALUE |
|---|---|---|---|---|---|---|
| PMH Information | [M] | [M] | [M] | [M] | [M] | [M] |
| Service values | [M] | [M] | [M] | [B] | [B] | [M] |
| System Category | | | | | | [M] |

Analysing the assigned levels, it is determined that the category of the information system is MEDIUM.

It should be noted that the determination of the category of the information system does not alter the security level of the individual dimensions, these individual dimensions being relevant when determining the applicability of certain measures of Annex II of Royal Decree 311/2022. This casuistry will be exemplified in the following sections of this guide..

# 4.2. Determination of the Declaration of Applicability

**Example 1.** If it is an information system with the following levels in each security dimension:

| SYSTEM 1 | | |
|---|---|---|
| **LEVELS OF SECURITY DIMENSIONS** | CONFIDENTIALITY (C) | **High** |
| | INTEGRITY (I) | **High** |
| | AVAILABILITY (D) | **Medium** |
| | AUTHENTICITY (A) | **High** |
| | TRACEABILITY (T) | **Low** |

Its category corresponds to the highest level associated with one of the dimensions. Therefore, the **category of this system is HIGH: [D(M), I(A), C(A), A(A), T(B)]**.

The measures to be applied are those required for High level except those that only apply to traceability (Medium or High level) and availability (High level).

That is, due to the traceability of Low Level, the measure [mp.info.4], marked as 'NOT APPLICABLE', will not be applicable. On the other hand, due to the availability of Medium Tier, measures [op.cont.2], [op.cont.3] and [op.cont.4] are not applicable, while in [mp.s.4] only the **baseline requirement** applies and in [mp.info.6] only the **mandatory reinforcement** R1 applies.

The statement of applicability will therefore be as follows:

**The measures to be applied are those required for High level except those that only apply to traceability (Medium or High level) and availability (High level).**

| CODE | DESCRIPTION | DIMENSIONS | SYSTEM CATEGORY |
|---|---|---|---|
| ORG | ORGANISATIONAL FRAMEWORK | | |
| org.1 | Security policy | D I C A T | applies |
| org.2 | Safety regulations | D I C A T | applies |
| org.3 | Security procedures | D I C A T | applies |
| org.4 | Authorisation process | D I C A T | applies |
| | OPERATIONAL FRAMEWORK | | |
| op.pl | Planning | | |
| op.pl.1 | Risk analysis | D I C A T | +R2 |
| op.pl.2 | Security Architecture | D I C A T | +R1 +R2 +R3 |
| op.pl.3 | Procurement of new components | D I C A T | applies |
| op.pl.4 | Sizing/capacity management | D _ _ _ _ | +R1 |
| op.pl.5 | Certified components | D I C A T | applies |
| op.acc | Access control | | |
| op.acc.1 | Identification | _ _ _ A T | +R1 |
| op.acc.2 | Access requirements | _ I C A T | +R1 |
| op.acc.3 | Segregation of duties and tasks | _ I C A T | +R1 |
| op.acc.4 | Access rights management process | _ I C A T | applies |
| op.acc.5 | Authentication mechanism (external users) | _ I C A T | + [R2 o R3 o R4] + R5 |
| op.acc.6 | Authentication mechanism (organisation's users) | _ I C A T | + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9 |
| op.exp | Exploitation | | |
| op.exp.1 | Inventory of assets | D I C A T | applies |
| op.exp.2 | Security settings | D I C A T | applies |
| op.exp.3 | Security configuration management | D I C A T | +R1 +R2 +R3 |
| op.exp.4 | Maintenance and security updates | D I C A T | +R1 +R2 |
| op.exp.5 | Change management | D I C A T | +R1 |
| op.exp.6 | Protection against malicious code | D I C A T | +R1 +R2 +R3 +R4 |
| op.exp.7 | Incident management | D I C A T | +R1 +R2 +R3 |
| op.exp.8 | Registration of the activity | _ _ _ _ T | applies |
| op.exp.9 | Incident management log | D I C A T | applies |
| op.exp.10 | Cryptographic key protection | D I C A T | +R1 |
| op.ext | External resources | | |
| op.ext.1 | Contracting and service level agreements | D I C A T | applies |
| op.ext.2 | Daily management | D I C A T | applies |
| op.ext.3 | Supply chain security | D I C A T | applies |
| op.ext.4 | Interconnection of systems | D I C A T | +R1 |

| CODE | DESCRIPTION | DIMENSIONS | SYSTEM CATEGORY |
|---|---|---|---|
| ORG | ORGANISATIONAL FRAMEWORK | | |
| op.nub | Cloud services | | |
| op.nub.1 | Protection of cloud services | D I C A T | +R1 +R2 |
| op.cont | Continuity of service | | |
| op.cont.1 | Impact analysis | D _ _ _ _ | applies |
| op.cont.2 | Continuity plan | D _ _ _ _ | n.a. |
| op.cont.3 | Periodic testing | D _ _ _ _ | n.a. |
| op.cont.4 | Alternative media | D _ _ _ _ | n.a. |
| op.mon | System monitoring | | |
| op.mon.1 | Intrusion detection | D I C A T | +R1 +R2 |
| op.mon.2 | Metrics system | D I C A T | +R1 +R2 |
| op.mon.3 | Surveillance | D I C A T | +R1 +R2 +R3 +R4 +R5 +R6 |
| | PROTECTION MEASURES | | |
| mp.if | Protection of installations and infrastructure | | |
| mp.if.1 | Separate and access-controlled areas | D I C A T | applies |
| mp.if.2 | Identification of persons | D I C A T | applies |
| mp.if.3 | Fitting out the premises | D I C A T | applies |
| mp.if.4 | Electric power | D _ _ _ _ | +R1 |
| mp.if.5 | Fire protection | D _ _ _ _ | applies |
| mp.if.6 | Flood protection | D _ _ _ _ | applies |
| mp.if.7 | Check-in and check-out of equipment | D I C A T | applies |
| mp.per | Personnel management | | |
| mp.per.1 | Job characterisation | D I C A T | applies |
| mp.per.2 | Duties and obligations | D I C A T | +R1 |
| mp.per.3 | Awareness-raising | D I C A T | applies |
| mp.per.4 | Training | D I C A T | applies |
| mp.eq | Protection of equipment | | |
| mp.eq.1 | Uncluttered workstation | D I C A T | +R1 |
| mp.eq.2 | Workplace blocking | _ _ _ A _ | +R1 |
| mp.eq.3 | Protection of portable devices | D I C A T | +R1 +R2 |
| mp.eq.4 | Other devices connected to the network | _ _ C _ _ | +R1 |
| mp.com | Protection of communications | | |
| mp.com.1 | Secure perimeter | D I C A T | applies |
| mp.com.2 | Protection of confidentiality | _ _ C _ _ | +R1 +R2 +R3 |
| mp.com.3 | Protection of integrity and authenticity | _ I _ A _ | +R1 +R2 +R3 +R4 |
| mp.com.4 | Separation of information flows in the network | D I C A T | +[R2 o R3] +R4 |

| CODE | DESCRIPTION | DIMENSIONS | SYSTEM CATEGORY |
|---|---|---|---|
| ORG | ORGANISATIONAL FRAMEWORK | | |
| mp.si | Protection of information media | | |
| mp.si.1 | Marking of supports | _ _ C _ _ | applies |
| mp.si.2 | Cryptography | _ I C _ _ | +R1 +R2 |
| mp.si.3 | Custody | D I C A T | applies |
| mp.si.4 | Transport | D I C A T | applies |
| mp.si.5 | Deletion and destruction | _ _ C _ _ | +R1 |
| mp.sw | Protection of computer applications | | |
| mp.sw.1 | Application development | D I C A T | +R1 +R2 +R3 +R4 |
| mp.sw.2 | Acceptance and commissioning | D I C A T | +R1 |
| mp.info | Protection of information | | |
| mp.info.1 | Personal data | D I C A T | applies |
| mp.info.2 | Qualification of information | _ _ C _ _ | applies |
| mp.info.3 | Electronic signature | _ I _ A _ | +R1 +R2 +R3 +R4 |
| mp.info.4 | Time stamps | _ _ _ _ T | n.a. |
| mp.info.5 | Cleaning of documents | _ _ C _ _ | applies |
| mp.info.6 | Back-up copies | D _ _ _ _ | +R1 |
| mp.s | Protection of services | | |
| mp.s.1 | Protection of electronic mail | D I C A T | applies |
| mp.s.2 | Protection of web services and applications | D I C A T | +R2 +R3 |
| mp.s.3 | Web browsing protection | D I C A T | +R1 |
| mp.s.4 | Denial of service protection | D _ _ _ _ | applies |

As a summary, from the 73 measures defined in Annex II of Royal Decree 311/2022, only 69 are applicable/required for the example system:

- 61 are applicable with a High level of stringency.
- 7 are applicable with a Medium level of stringency.
- 1 is applicable with a Low requirement level.
- 4 do not apply.

# 5. Specific compliance profile

We can define a Specific Compliance Profile (SCP) as the set of security measures, whether included in Annex II of RD 311/2022, which, as a result of the mandatory risk analysis, are applicable to a specific entity or sector of activity and for a specific security category.

The CCN, in the exercise of its competences, shall validate and publish the corresponding specific compliance profiles that are defined, together with the corresponding accreditation and validation frameworks, according to the technical security instructions and security guides approved according to the provisions of the second additional provision of the ENS.

Consequently, when preparing the Statement of Applicability for a particular Information System, an organisation should assess whether it is eligible for a SCP and, if so, adapt the Statement of Applicability to it.

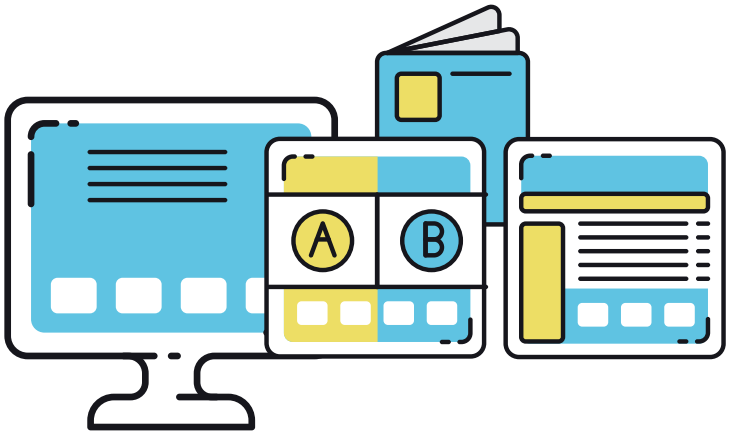
**When preparing the Statement of Applicability for a particular Information System, an organisation should assess whether it is eligible for a SCP and, if so, adapt the Statement of Applicability to it**

# 6. Recommendations

## 6.1. Regarding the format of the Declaration of Applicability

For clarity and usefulness of the Statement of Applicability, it is good practice to add two (2) additional columns: the **degree of implementation** of each of the applicable measures (CCN-STIC-808), as well as the **maturity level** with a brief description of how each measure applies in the Organisation's Information System.

In that description, if any security measure (whether complete or its basic reinforcement or possible mandatory reinforcement) has been replaced by a **compensatory measure**, a reference to the compensatory measure will be included. The same will apply if **supplementary supervision measures** are used for a particular security measure.



| DECLARATION OF APPLICABILITY RD 311/2022 | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| DIMENSION | B | M | A | Measure | Description | Appli-cation | Degree Implemen. | Maturity level | DETAIL OF HOW IT APPLIES, OR WHY IT APPLIES |
| ORGANISATIONAL FRAMEWORK | | | | | | | | | |
| Category | APL | APL | APL | org.1 | Security Policy | Yes | G2 | L3 | The document "POL-001 Security Policy" is available and the latest version is referenced in the version control as V1.1 dated 24/10/2022. It has been communicated internally in the organisation through the intranet. |
| Category | APL | APL | APL | org.2 | Safety regulations | Yes | G2 | L3 | The document "NOR-001 System Usage Policy", which develops the Security Policy, is available. The regulations for the use of the systems have been subscribed by the employees of the organisation, signing the final blank. |
| Category | APL | APL | = | org.3 | Security Procedure | Yes | G2 | L1 | |
| Category | APL | APL | APL | org.4 | Authorisation process | Yes | G2 | L1 | |
| OPERATIONAL FRAMEWORK | | | | | | | | | |
| | | | | op.pl. | PLANNING | | | | |
| Category | APL | +R1 | +R2 | op.pl.1 | Risk analysis | Yes | G2 | L2 | |
| Category | APL | +R1 | +R1 +R2 +R3 | op.pl.2 | Security Architecture | Yes | G2 | L2 | |
| Category | APL | APL | APL | op.pl.3 | Procurement of new components | Yes | G2 | L2 | |
| D | APL | +R1 | +R1 | op.pl.4 | Capacity management | Yes | G0 | L0 | |
| Category | N/A | APL | APL | op.pl.5 | Certified components | NO | | | NOT APPLICABLE AS THIS IS A MEASURE FOR MEDIUM AND HIGH CATEGORY SYSTEMS |

It can be seen in the example extract in the figure above, which represents a BASIC category system, how the concrete applicability is described for measures [org.1] and [org.2]. In the column 'Degree of implementation', G0 means that the measure is not implemented, G1 that it is in the process of implementation and G2 that it is implemented.

Illustration 2. Extract from a possible Statement of Applicability.

# 6.2. Decalogue of general recommendations

Below is a decalogue of recommendations to be taken into account in order to determine a Statement of Applicability within the scope of the National Security Framework.

| DECALOGUE OF RECOMMENDATIONS FOR THE DECLARATION OF APPLICABILITY (DOA) | |
|---|---|
| 1 | First of all, value the essential assets (of the "Information" and "Service" types). |
| 2 | To assess the assets, determine the security level for each of the dimensions: confidentiality [C], integrity [I], availability [D], authenticity [A] and traceability [T]. This level shall be determined according to the consequences of a security incident on one of the dimensions. |
| 3 | If the essential asset is of the "Service" type, it is recommended to first assess the availability dimension [D], as the requirements for confidentiality, integrity, authenticity and traceability are usually inherited from the assessment of "Information" type assets. |
| 4 | Establish the category of the system (BASIC, MEDIUM or HIGH) according to the security levels assigned to the different dimensions, taking into account that assigning a category to the system requires setting a degree of implementation of the measures to be applied and that the category of the system will be the highest of the security levels assigned. |
| 5 | Select the measures that apply to the system according to their category, out of a total of 45 measures. |
| 6 | Select the measures that apply to the system according to their security levels, out of a total of 28 measures. |

| | |
|---|---|
| 7 | Use the simulator developed by CCN-CERT, which helps to determine the Statement of Applicability automatically, entering the security levels for each of the dimensions of the asset. |
| 8 | Indicate in detail the correspondence between the compensatory measures implemented and the Annex II measures they compensate for; similarly for any additional surveillance measures. The whole shall be formally approved by the Security Officer. |
| 9 | If any compensatory measures are included in the Statement of Applicability, please detail, for each of them, the following parameters: scope of application, limitations or restrictions, objective, identified risk, definition of the compensatory measure, validation of the compensatory measure and maintenance. The content of these parameters is set out in Guide CCN-STIC-819 Compensatory Measures. |
| 10 | For the drafting of the Statement of Applicability document, use a self-drafted document or the template developed by CCN-CERT, taking into account the compliance profiles validated by the CCN in the corresponding CCN-STIC guides. |

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es