centro criptológico nacional

ICT Security Guide
CCN-STIC 140
ENGLISH EDITION

Reference taxonomy for ICT Security Products and Services

COURTESY TRANSLATION OF CCN-STIC 140 (SPANISH EDITION: SEPTEMBER 2023)

September 2025

MINISTERIO DE DEFENSA

Catalog of Publications of the General Administration of the State
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
Pº de la Castellana 109, 28046 Madrid
National Cryptologic Center, 2025

NIPO: 083-25-181-4
Release Date: September 2025

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.29 11:40:41 +01'00'

INDEX

1. INTRODUCTION 5
2. OBJECTIVE 9
3. SCOPE 10
4. TAXONOMY OF QUALIFIED PRODUCTS 11
4.1 TAXONOMY: STRUCTURE 11
4.2 TAXONOMY: SCHEME 11
4.3 TAXONOMY: DESCRIPTION 17
4.3.1. ACCESS CONTROL 17
4.3.1.1. CATEGORY: NETWORK ACCESS CONTROL (NAC) 17
4.3.1.2. CATEGORY: BIOMETRIC DEVICES 18
4.3.1.3. CATEGORY: *SINGLE SIGN-ON* DEVICES 18
4.3.1.4. CATEGORY: AUTHENTICATION SERVERS 18
4.3.1.5. CATEGORY: *ONE-TIME PASSWORD* DEVICES 18
4.3.1.6. CATEGORY: PRIVILEGED ACCESS MANAGEMENT (PAM) 18
4.3.1.7. CATEGORY: IDENTITY MANAGEMENT (IM) 18
4.3.2. SAFETY IN THE EXPLOITATION 18
4.3.2.1. CATEGORY: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM) 19
4.3.2.2. CATEGORY: EDR (ENDPOINT DETECTION AND RESPONSE) 19
4.3.2.3. CATEGORY: NETWORK MANAGEMENT TOOLS 19
4.3.2.4. CATEGORY: SYSTEMS UPDATE TOOLS 19
4.3.2.5. CATEGORY: NAVIGATION FILTERING TOOLS 19
4.3.2.6. CATEGORY: SECURITY EVENT MANAGEMENT SYSTEMS (SIEM) 19
4.3.2.7. CATEGORY: DEVICES FOR CRYPTOGRAPHIC KEY MANAGEMENT 20
4.3.2.8. CATEGORY: DEVICE MANAGEMENT TOOLS (UEM) 20
4.3.2.9. CATEGORY: ORCHESTRATION, AUTOMATION AND SAFETY RESPONSE (SOAR) SYSTEMS 20
4.3.3. SAFETY MONITORING 20
4.3.3.1. CATEGORY: IPS, IDS AND ANTIDDOS DEVICES 20
4.3.3.2. CATEGORY: HONEYPOT / HONEYNET SYSTEMS 20
4.3.3.3. CATEGORY: TRAFFIC CAPTURE, MONITORING AND ANALYSIS 21
4.3.3.4. CATEGORY: SANDBOX TOOLS 21
4.3.4. PROTECTION OF COMMUNICATIONS 21
4.3.4.1. CATEGORY: ROUTERS 21
4.3.4.2. CATEGORY: *SWITCHES* 21
4.3.4.3. CATEGORY: FIREWALLS 21
4.3.4.4. CATEGORY: *PROXIES* 22
4.3.4.5. CATEGORY: WIRELESS NETWORK DEVICES 22
4.3.4.6. CATEGORY: SECURE DATA EXCHANGE GATEWAYS 22
4.3.4.7. CATEGORY: DATA DIODES 22
4.3.4.8. CATEGORY: VIRTUAL PRIVATE NETWORKS 22
4.3.4.9. CATEGORY: VOICE AND VIDEO OVER IP (VVOIP) TOOLS 22
4.3.4.10. CATEGORY: INSTANT MESSAGING (IM) TOOLS 23

4.3.4.11. CATEGORY: VIDEOCONFERENCING TOOLS 23
4.3.4.12. CATEGORY: WEB APPLICATION FIREWALL (WAF)....23
4.3.4.13. CATEGORY: *SOFTWARE* DEFINED NETWORKS (SDN) 23
4.3.5. PROTECTION OF INFORMATION AND INFORMATION MEDIA 23
4.3.5.1. CATEGORY: ENCRYPTED DATA STORAGE 23
4.3.5.2. CATEGORY: ENCRYPTION AND SECURE SHARING OF INFORMATION....23
4.3.5.3. CATEGORY: SECURE ERASE TOOLS 24
4.3.5.4. CATEGORY: DATA LEAK PREVENTION SYSTEMS 24
4.3.5.5. CATEGORY: TOOLS FOR ELECTRONIC SIGNATURE 24
4.3.5.6. CATEGORY: *HARDWARE SECURITY MODULE* (HSM) 24
4.3.5.7. CATEGORY: METADATA MANAGEMENT 24
4.3.6. PROTECTION OF EQUIPMENT AND SERVICES 24
4.3.6.1. CATEGORY: MOBILE DEVICES 24
4.3.6.2. CATEGORY: OPERATING SYSTEMS....25
4.3.6.3. CATEGORY: EMAIL PROTECTION 25
4.3.6.4. CATEGORY: SMART CARDS 25
4.3.6.5. CATEGORY: BACKUPS 25
4.3.6.6. CATEGORY: RELIABLE PLATFORMS 25
4.3.6.7. CATEGORY: VIRTUALIZATION 25
4.3.6.8. CATEGORY: LOAD BALANCERS....25
4.3.6.9. CATEGORY: CASB 26
4.3.6.10. CATEGORY: HYPERCONVERGENCE....26
4.3.6.11. CATEGORY: VIDEOIDENTIFICATION TOOLS....26
4.3.6.12. CATEGORY: VIRTUAL DESKTOP INFRASTRUCTURE (VDI) 26
4.3.6.13. CATEGORY: KVM SWITCHES....26
4.3.6.14. CATEGORY: DATABASE MANAGEMENT SYSTEMS (DBMS) 26
4.3.7. PROTECTION OF INSTALLATIONS AND INFRASTRUCTURES 27
4.3.7.1. CATEGORY: IP CAMERAS....27
4.3.7.2. CATEGORY: VIDEO MANAGEMENT 27
4.3.8. SAFETY OT....27
4.3.8.1. CATEGORY: ELECTRIC VEHICLE CHARGING STATIONS....27
4.3.9. CLOUD SECURITY SERVICES 27
4.3.10. OTHER TOOLS 27
4.3.11. TOOLS FOR THE DEVELOPMENT OF SAFETY PRODUCTS....27
5. TAXONOMY OF APPROVED PRODUCTS 28
5.1 CATEGORY: PROTECTION IN TACTICAL ENVIRONMENTS 28
5.1.1. CATEGORY: RELIABLE TACTICAL PLATFORMS AND DEVICES 29
5.1.2. CATEGORY: SOLUTIONS TO PROTECT TACTICAL COMMUNICATIONS....29
5.1.3. CATEGORY: INFORMATION SYSTEMS FOR TACTICAL ENVIRONMENTS....30
6. TAXONOMY OF PRODUCTS AND SERVICES OF COMPLIANCE AND SECURITY GOVERNANCE 31
6.1 CATEGORY: GOVERNANCE AND SECURITY PLANNING 31
6.2 CATEGORY: SAFETY AND COMPLIANCE REGULATIONS 31
6.3 CATEGORY: RISK ANALYSIS AND MANAGEMENT 31
6.4 CATEGORY: NOTIFICATION AND MANAGEMENT OF CYBER INCIDENTS 32

6.5 CATEGORY: CYBERINTELLIGENCE EXCHANGE 32
6.6 CATEGORY: TRAINING AND AWARENESS IN CYBERSECURITY 32
7. REFERENCES 33
8. ABBREVIATIONS 34

1. INTRODUCTION

1. The acquisition of an ICT security product that will handle classified national information or sensitive information should be preceded by a process of verification that the security mechanisms implemented in the product are adequate to protect such information.
2. The evaluation and certification of an ICT security product is the only objective means to assess and prove the ability of a product to handle information securely. In Spain, this responsibility is assigned to the National Cryptologic Center (CCN) through RD 421/2004 of 12 March in its article 1 and in its article 2.1, which establishes that the Director of the CCN is the certification authority of the security of information and communications technologies and the authority of cryptological certification.
3. Likewise, within the RD 311/2022 of 3 May, which regulates the National Security Scheme (ENS) in the field of Electronic Administration, it is indicated that the CCN Certification Body will be responsible for determining the requirements for each ICT Security product or service for additional certifications and/or evaluations.
4. Based on these competencies, the CCN publishes the **CCN-STIC 105** Guide **Catalog of Information and Communication Technology Security Products and Services (CPSTIC)** [1]. This catalog aims to offer to the agencies of the Administration a set of products or services STIC of reference, whose security functionalities related to the object of their acquisition have been certified.
5. In this way, the CPSTIC allows to provide a minimum level of confidence to the end user in the products or services purchased, based on the safety improvements derived from the evaluation and certification process and on a safe use procedure.
6. CPSTIC consists of three (3) parts: Approved Products, Qualified Products and Services, and Compliance and Safety Governance Products and Services[1].
7. The **Approved Products** section includes those products that are considered suitable for handling classified information.
8. The **Qualified Products** section includes those that meet the safety requirements required for handling sensitive information in the ENS, in any of its categories (HIGH, MEDIUM and BASIC).
9. The **Compliance and Security Governance Products** section includes governance and security planning tools, regulatory and compliance tools and, finally, risk analysis and management tools. These are products that do not fit into the product categories defined in the taxonomy of approved and qualified products, since they are products that do not belong to the security architecture of the system.

[1] Although CPSTIC collects Qualified Products and Services or Products and Services of Compliance and Security Governance, by language economy, from now on we will talk about Qualified Products or Products **of Compliance and Security Governance** .

TYPE OF PRODUCT OR SERVICE	INFORMATION YOU HANDLE
APPROVED	CLASSIFIED
QUALIFIED	SENSITIVE (ENS)
SECURITY COMPLIANCE AND GOVERNANCE	ANY KIND

Table 1. Types of products included in the CPSTIC

10. For the inclusion of a product in the catalog, the CCN shall take into account the following criteria:

    a) In the case **of products approved** for the handling of classified information, the highest level of classification of the information that can be handled (DIFUSION LIMITADA, CONFIDENCIAL, RESERVADO, SECRETO).

    b) In the case of **qualified products** , the highest category of the information system in which it can be used (HIGH, MEDIUM, BASIC[2]).

    c) The security functionalities that the product implements and the certifications provided.

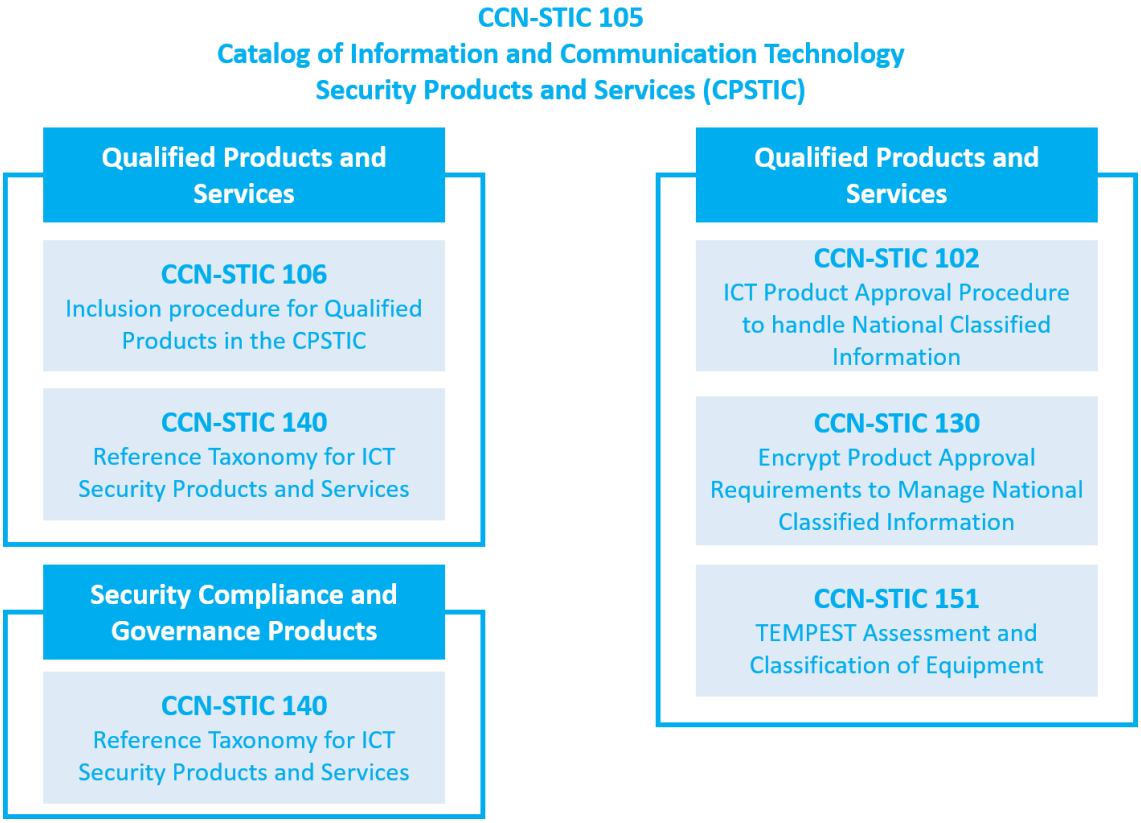
    d) Other aspects such as the risk analysis of the product or system, the operational need within the Administration, the availability or not of other certified products that satisfy the same functionality, etc.

11. Based on this information, the tests or evaluations to be passed by the relevant ICT security product will be determined.

12. The procedure for the inclusion in the CPSTIC of an approved STIC product to handle national classified information is described in the **CCN-STIC 102** Guidance **Procedure for the Approval of ICT Security Products to Handle National Classified Information** [2]. The required requirements, the list of documentation and equipment to be provided to perform the cryptological evaluation is described in **CCN-STIC 130 Encrypt Product Approval Requirements to Manage National Classified Information** [3] And to perform the TEMPEST evaluation is described in the **CCN-STIC 151** Guide **TEMPEST Assessment and Classification of Equipment** [4].

[2] Classification by categories defined in the ENS.

See



13. Figure 1. CPSTIC Classification

14. Likewise, the procedure for the inclusion of an approved STIC product in the CPSTIC to handle classified national information is described in the **CCN-STIC 102 Guide Procedure for the Approval of ICT Security Products to Handle National Classified Information** [2]. The required requirements, the relationship of documentation and equipment to be provided to perform the cryptological evaluation are described in CCN-STIC 130 Encrypa Product Approval Requirements to Manage National Classified Information [3] And to perform the TEMPEST evaluation is described in the CCN-STIC 151 Guide TEMPEST Assessment and Classification of Equipment [4]. See **¡Error! No se encuentra el origen de la referencia.**.

15. The STIC product or service qualified or approved by the CCN shall refer to a specific version and with a certain configuration, according to rules of use which shall be described in a Safe Use Procedure (SSP). This PES will be distributed by the manufacturer along with the product and will also be published as a CCN-STIC guide to the 1000 series.

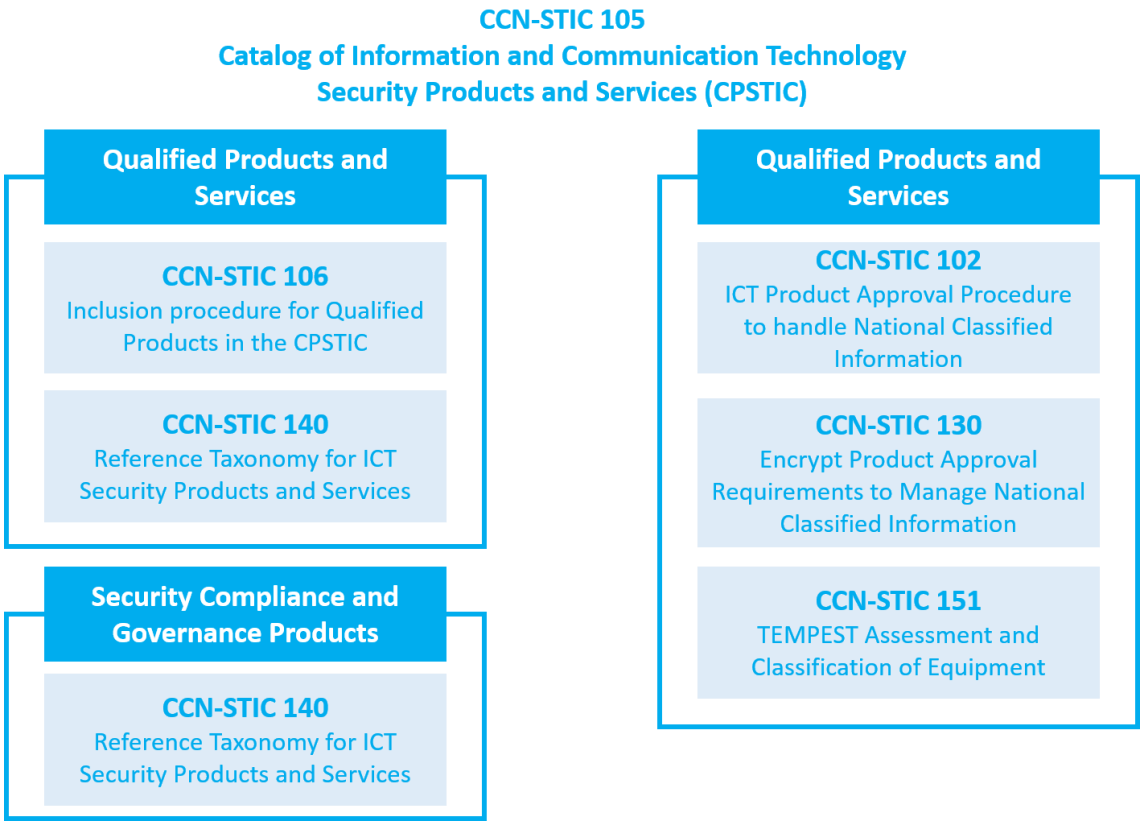


Figure 1. CPSTIC Classification

2. OBJECTIVE

16. The purpose of this document is to establish a taxonomy for the classification of Security Products in Information and Communication Technologies (ICT) around different categories, and identify their scope and scope, in order to serve as a basis for classifying products included in the CPSTIC.

17. In addition, each of the Annexes to this document includes the Basic Safety Requirements (RFS), defined for each category, which will be required for each product that wishes to be included in the CPSTIC.

3. SCOPE

18. The taxonomy described in this document is divided into three (3) parts. The first two (**Taxonomy of Qualified and Approved Products and Services**) establish a classification of those ICT products that are part of the security architecture of ICT systems, that is, those that develop their activity in the operational context of ICT systems, and implement functionalities that allow to increase the level of security of the system in some of its dimensions (availability, integrity, confidentiality, authenticity and traceability).

19. Also included will be products whose main functionality is not related to security but that do implement critical security features within the system, such as routers, operating systems, mobile devices, etc.

20. The third part (**Taxonomy of Compliance Products and Services and Security Governance**) shall include products that are not covered by the two preceding ones, as they are not part of the security architecture of the system, but they implement functionalities that facilitate compliance with security regulations. In this group would be, for example, auditing tools, risk analysis or bastioning of systems/equipment.

21. The products included in each category of the taxonomy may be implemented, unless expressly indicated otherwise, in hardware equipment, *software* application or logic for integrated circuits (*firmware)*.

4. TAXONOMY OF QUALIFIED PRODUCTS

4.1 TAXONOMY: STRUCTURE

22. In order for the Catalog to serve as a reference instrument to meet the needs of the Public Administration to comply with safety regulations and, in particular, with the National Security Scheme (ENS), the structure of the taxonomy is organized based on the security measures defined in Annex II of Royal Decree 311/2022 of 3 May regulating the National Security Scheme (ENS) in the field of Electronic Administration[3] .

23. The taxonomy is divided into categories that have been defined, with the intention of adapting to future changes that may occur in the market of STIC products

24. A category groups security products based on their basic functionality (e.g. router, firewall, proxy, secure erase tool, etc.). These products may contribute to the implementation of some of the safety requirements contained in the measures in Annex II of the ENS. These measures are referenced next to each category by their identifier (e.g. [op.exp.N] covers the "N" requirement of exploitation measures within the operational framework).

25. According to this structure, it could be the case that a product falls into one or several complementary categories provided that it implements the functionalities of all of them. This is becoming increasingly common, as companies developing security products tend to take an *all-in-one* approach through application packages or dedicated equipment (*suites/appliances*) that cover various security functionalities in a single device or system.

26. For each category of taxonomy products a document of Fundamental Safety Requirements (RFS) has been defined, which should be taken as a reference for the development, evaluation and safe use of products within each category. These RFS are included in the annexes to this guide.

4.2 TAXONOMY: SCHEME

27. The Table 2 includes the scheme of the taxonomy organized based on the security measures set out in Annex II of the ENS in which the products associated with each category could contribute to its compliance, as well as the list of annexes to this document, where the Fundamental Safety Requirements (RFS) required for each category of products are collected and depending on the category of the system (MEDIUM or HIGH) in which they are to be used.

[3] https://www.boe.es/eli/es/rd/2022/05/03/311

CATEGORIES				
SECURITY MEASURES	NAME	MEASURES	ANNEXES	
			ENS HIGH	MEDIUM ENS
Access control [op.acc]	Network Access Control (NAC[4])	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.1	A.1M
	Biometric devices	[op.acc.1]; [op.acc.2]; [op.acc.5]	A.2	
	Single Sign-On devices	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.3	
	Authentication servers	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.4	A.4M
	One-Time Password devices	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.5 (*)	
	Privileged Access Management (PAM[5])	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A.6	A.6M
	Identity Management (IM[6])	[op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.acc.7]	A7	A.7M

[4] *Network Access Control*
[5] *Privileged Access Manager*
[6] *Identity Management*

CATEGORIES				
SECURITY MEASURES	NAME	MEASURES	ANNEXES	
			ENS HIGH	MEDIUM ENS
Operational Safety [op.exp]	Anti-Virus/EPP (*Endpoint Protection Platform*)	[op.exp.6]	B.1	B.1M
	EDR (*Endpoint Detection and Response)*	[op.exp.6]	B.2	B.2M
	Network management tools	[op.exp.3]; [op.exp.7]	B.3	B.3M
	Systems update tools	[op.exp.4]; [op.exp.5]	B.4	
	Navigation filtering tools	[op.exp.6]	B.5	B.5M
	Security Event Management Systems (SIEM)	[op.exp.8]; [op.exp.9]; [op.exp.10]	B.6	B.6M
	Devices for cryptographic key management	[op.exp.11]	B.7(*)	NA
	Device Management Tools (UEM)	[op.exp.3]	B.8	NA
	Orchestration, Automation and Safety Response (SOAR) Systems	[op.exp.8]; [op.exp.9];	B.9	B.9M
Security monitoring [op.mon]	IDs, IPS and AntiDDoS	[op.mon.1]	C.1	C.1M
	Honeypot / Honeynet systems	[op.mon.1]	C.2	
	Traffic capture, monitoring and analysis	[op.mon.1]	C.3	C.3M
	Sandbox tools	[op.mon.1]	C.4	C.4M
	Routers	[mp.com.3]; [mp.com.4]	D.1	D.1M

CATEGORIES				
SECURITY MEASURES	NAME	MEASURES	ANNEXES	
			ENS HIGH	MEDIUM ENS
Protection of communications [mp.com]	Switches	[mp.com.4]	D.2	D.2M
	Firewalls	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.3	D.3M
	Proxies	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.4	D.4M
	Wireless Network Devices	[mp.com.3]; [mp.com.4]	D.5	D.5M
	Secure data exchange gateways	[mp.com.4]	D.6	NA
	Data diodes	[mp.com.4]	D.7	NA
	Virtual private networks – IPsec	[mp.com.2]; [mp.com.3]	D.8A	
	Virtual private networks – TLS		D.8B	
	Voice and video tools over IP (VVoIP)	[mp.com.2]; [mp.com.3]	D.9A	D.9AM
	Instant Messaging (IM) Tools		D.9B	D. 9BM
	Video conferencing tools		D.9C	D.9CM
	Web Application Firewall (WAF)	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.10	D.10
	Networks defined by *Software* (SDN)	[mp.com.1]; [mp.com.3]; [mp.com.4]	D.11	
Information Protection [mp.info] and	Encrypted data storage	[mp.si.2]; [mp.info.3]	E.1	
	Encryption and secure sharing of information	[mp.si.2]; [mp.info.3]	E.2	

CATEGORIES				
SECURITY MEASURES	NAME	MEASURES	ANNEXES	
			ENS HIGH	MEDIUM ENS
Information Media [mp.si]	Secure erasure tools	[mp.si.5]	E.3	E.3M
	Data leak prevention systems	[mp.info.2]	E.4	
	Tools for electronic signature	[mp.info.4]; [mp.info.5]	E.5	NA
	Hardware Security Module (HSM)	[mp.si.2]; [mp.info.3]	E.6	NA
	Metadata management	[mp.si.1]; [mp.info.5] Transversely: [op.mon.3]	E.7	E.7M
Protection of Equipment [mp.eq] and Services [mp.s]	Mobile devices	[mp.eq.3]	F.1	NA
	Operating systems	[mp.eq.2] Transversely: [op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	F.2	NA
	Email protection	Transversely: [op.acc.1]; [op.acc.5]; [mp.SI.2]	F.3	F.3M
	Smart cards	[mp.1]	F.4	NA
	Backup copies	[mp.info.9]	F.5	
	Reliable platforms	[mp.eq.2] Transversely: [Op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	F.6	

CATEGORIES				
SECURITY MEASURES	NAME	MEASURES	ANNEXES	
			ENS HIGH	MEDIUM ENS
	Virtualization	[mp.eq.2] Transversely: [Op.acc.1]; [op.acc.2]; [op.acc.5]; [op.acc.6]; [op.exp.8]	F.7	F.7M
	Load balancers	[mp.8]	F.8	F.8M
	CASB	[mp.s] Transversely: [mp.info]; [mp.acc]; [op.exp.2]	F.9	F.9M
	Hyperconvergence	[mp.s] Transversely: [mp.com]; [op.cont] [mp.info.9]	F.10	F.10M
	Video identification tools	[mp.2]	F.11	F.11M
	Virtual Desktop Infrastructure (VDI)	[op.acc.4] [op.acc.6] [mp.eq.3] [mp.si]	F.12	F.12M
	KVM switches		F.13	
	Database Management Systems (DBMS)	Control and access requirements. Security configuration Inventory of assets Maintenance and security updates	F.14	
	IP cameras	[mp.if]	I.1	I.1M

CATEGORIES				
SECURITY MEASURES	NAME	MEASURES	ANNEXES	
			ENS HIGH	MEDIUM ENS
Protection of facilities and infrastructure [mp.if]	Video management	[mp.if]	I.2	I.2M
Safety OT	Electric vehicle charging stations			O.1M
Cloud security services		-	G	
Other tools		-	-	
Tools for the development of safety products		-	-	

Table 2. Taxonomy of Qualified Products and Services

Note: The annexes marked with (*) are in preparation at the date of publication of this guide. The RFS corresponding to these categories will be published in future versions.

4.3 TAXONOMY: DESCRIPTION

4.3.1. ACCESS CONTROL

28. Every body needs the ability to have different user profiles and, in turn, each user has personalized access credentials. These capabilities, coupled with appropriate security policies for each type of user, allow control of access to available resources. It covers all product categories that facilitate these capabilities.

4.3.1.1. CATEGORY: NETWORK ACCESS CONTROL (NAC)

29. It encompasses all products that have mechanisms for the administration and access of a set of users to a specific network. Among its configuration options, they have specific security solutions to increase or decrease network availability and thus achieve regulatory compliance of the company or agency.

4.3.1.2. CATEGORY: BIOMETRIC DEVICES

30. They allow authentication and identification of users by presenting unique physical attributes such as fingerprint, eye iris, etc.

4.3.1.3. CATEGORY: *SINGLE SIGN-ON* DEVICES

31. They enable access to multiple systems within an organization by performing only one authentication, that is, it is not necessary to repeat the authentication process for each service, but only one access/account is sufficient.

4.3.1.4. CATEGORY: AUTHENTICATION SERVERS

32. The products associated with this category are primarily aimed at verifying the identity of a user or device within a protected network architecture based on one or more factors. These products are often placed right in front of an organization's services to ensure that they are only used by those identities authorized according to the organization's security policy.

4.3.1.5. CATEGORY: *ONE-TIME PASSWORD* DEVICES

33. The products associated with this category are primarily aimed at providing a means of generating single-use access keys, known as *tokens*, which serve to strengthen any authentication system or procedure, avoiding various attacks such as brute force and allowing to implement strong or multi-factor authentication strategies.

4.3.1.6. CATEGORY: PRIVILEGED ACCESS MANAGEMENT (PAM)

34. Products associated with this category allow privileged secure access to critical assets of a system according to an organization's policies. To do this, they manage and monitor privileged accounts and access: They discover privileged accounts, devices or applications; manage and protect credentials; control access to privileged accounts; and isolate and monitor privileged access sessions.

4.3.1.7. CATEGORY: IDENTITY MANAGEMENT (IM)

35. The *Identity Management* (*IM)* category products provide organizations with centralized and synchronized digital identity services. They generate a unique identity for each user, so that they can be uniquely identified, and to which to associate the rest of the attributes for authentication (credentials) and authorization (permissions), along with other attributes of interest.

4.3.2. SAFETY IN THE EXPLOITATION

36. Covers product categories that facilitate the management of security during the operation of a computer system, from its implementation and commissioning to its end of service; allowing to maintain a correct configuration of protection measures and security levels in your day to day.

4.3.2.1. CATEGORY: ANTI-VIRUS/EPP (ENDPOINT PROTECTION PLATFORM)

37. They focus on the prevention, detection and disinfection of computer viruses. As the Internet has grown and gained in popularity, these tools have progressed in line and are currently very advanced products, focused on preventing and preventing the spread by seeking that the systems where they run are not compromised by harmful codes of different nature.

4.3.2.2. CATEGORY: EDR (ENDPOINT DETECTION AND RESPONSE)

38. Because anti-virus or EPP tools do not provide complete protection, a new category of applications called EDR (*Endpoint Detection and Response*) has emerged that add security features focused on detecting and blocking unknown malware.

39. The functionality of EDR has evolved over time. In its original concept it was tools to monitor and observe the execution of processes. Currently EDR tools have evolved covering part of the EPP features and incorporating IR (*Incident Response*) functionalities, toward a new category called *the Next Generation Endpoint Protection Platform (NGEPP).*

4.3.2.3. CATEGORY: NETWORK MANAGEMENT TOOLS

40. They allow centrally to manage and configure the infrastructure of devices that make up a network, monitor their performance and resource consumption, as well as troubleshooting in the network.

4.3.2.4. CATEGORY: SYSTEMS UPDATE TOOLS

41. They allow the software components of a system to be updated in response to modifications and updates provided by the providers, mainly in order to correct security flaws or existing vulnerabilities, as well as to add new functionalities to the affected systems.

4.3.2.5. CATEGORY: NAVIGATION FILTERING TOOLS

42. They protect the user during Internet browsing. They control the websites and services that can be viewed or accessed. To achieve this, they make use of trusted or reputable lists based on URL addresses[7], as well as may limit all access to untrusted or potentially dangerous sites.

4.3.2.6. CATEGORY: SECURITY EVENT MANAGEMENT SYSTEMS (SIEM)

43. They support security monitoring by facilitating the process of collecting, analyzing and collecting, as well as safeguarding information on security events and anomalies that may indicate a commitment to security in systems, being able to additionally provide functionalities for the detection and notification of security

[7]**URL (*Uniform Resource Locator*):** Uniform location of the resource. It is the way a site is identified on the internet. EJ www.ccn.cni.es

incidents, and facilitating the traceability as fast and simple as possible of the events.

4.3.2.7. CATEGORY: DEVICES FOR CRYPTOGRAPHIC KEY MANAGEMENT

44. They allow to carry out the necessary control and safeguard of the cryptographic keys used for the protection of communications, as well as the information stored, throughout its life cycle, including its generation, transport, custody during its exploitation, subsequent archiving once removed and final destruction.

4.3.2.8. CATEGORY: DEVICE MANAGEMENT TOOLS (UEM)

45. They enable efficient management of diversity and massive, dynamic and large-scale deployment of devices in an organization. Device management tools allow you to apply security policies and configurations to the devices of an organization so that they can be used to process information according to the established criteria.

4.3.2.9. CATEGORY: ORCHESTRATION, AUTOMATION AND SAFETY RESPONSE (SOAR) SYSTEMS

46. The products or services associated with this category are aimed at incident management, task automation and response coordination. In addition, they provide alert processing and correlation capabilities, which together allow organizations faster detection and response to security incidents, minimizing impact and improving the overall security posture.

4.3.3. SAFETY MONITORING

47. The effective response to security incidents is based on the rapid detection and correct identification of activities that indicate a commitment to security in the systems. It covers product categories that allow continuous safety monitoring by automating the analysis of security events, the collection and reporting of safety information, and the possible reaction to detected incidents.

4.3.3.1. CATEGORY: IPS, IDS AND ANTIDDOS DEVICES

48. Its main function is to detect and prevent unauthorized access, either to a specific network or to a computer on which they are installed. To achieve their goal, they perform network traffic monitoring functions to determine and prevent suspicious behaviors.

4.3.3.2. CATEGORY: HONEYPOT / HONEYNET SYSTEMS

49. Attract and detect harmful activity in a simulated network or application that emulates systems of interest to an attacker, allowing the monitoring of their activities to subsequently improve the protection mechanisms of the real networks of the organization.

4.3.3.3. CATEGORY: TRAFFIC CAPTURE, MONITORING AND ANALYSIS

50. They allow the collection, display and analysis of network traffic facilitating the detection and investigation of possible security events, mainly related to the improper or unauthorized use of network protocols.

4.3.3.4. CATEGORY: SANDBOX TOOLS

51. They allow the execution of applications in an isolated and controlled way in order to analyze their execution and detect if they contain harmful code. In the event that the executed application contains *malware*, it is guaranteed that the system on which the *sandbox* tool is deployed is not infected.

4.3.4. PROTECTION OF COMMUNICATIONS

52. Englobaas Product categories whose main purpose is to protect communications established between systems and/or devices connected within a network. Its main functions include establishing a security perimeter, ensuring secure communications and preventing attacks from other external networks.

4.3.4.1. CATEGORY: ROUTERS

53. They provide network-level connectivity of the OSI model[8] , allowing to manage the routing or routing of data packets between different subnets. To do this, it will be necessary for the device to store the received packets, process their source and destination information, and finally forward them. They have specific functionalities for configuring and monitoring traffic, either locally or remotely.

4.3.4.2. CATEGORY: *SWITCHES*

54. Allow two or more network segments to be interconnected at the OSI data link level for the purpose of merging them into a single network; passing data from one segment to another according to the[9] destination MAC address of frames in the network and removing the connection once it is terminated.

4.3.4.3. CATEGORY: FIREWALLS

55. They control the flows of information between networks allowing the blocking of those accesses that have not been authorized. They also prevent the spread of malicious software between the network member computers they protect. They can work at different levels of the OSI layer and be deployed as dedicated *devices* or as software applications.

[8] **OSI (Open System Interconnection):** Open Systems Interconnection Model.
[9] **MAC (*Media Access Control*):** This is also known as the physical address of a card or network device and is unique to each card or network device. It consists of six groups of two hexadecimal characters separated by two points.

4.3.4.4. CATEGORY: *PROXIES*

56. They act as intermediaries in communications through interconnections between internal and external networks, accepting requests from clients of the protected network and acting on their behalf before external devices, masking and protecting the user against possible attackers.

4.3.4.5. CATEGORY: WIRELESS NETWORK DEVICES

57. They allow the connectivity of equipment and mobile devices to a network by wireless means (e.g. WiFi), via electromagnetic waves and without the need for access to a wired network. They should implement mechanisms so that remote communications between the wireless network device and the node connecting to it are not compromised.

4.3.4.6. CATEGORY: SECURE DATA EXCHANGE GATEWAYS

58. They allow the interconnection of networks avoiding the leakage of unauthorized information, both in the direction of input and output, by breaking the continuity of communications protocols and configuring an interface for certain types of data exchange services, such as e-mail, computer files, etc. allowing the transit of information in both directions, but without simultaneously using the same resources.

4.3.4.7. CATEGORY: DATA DIODES

59. They limit connectivity between teams/networks, allowing the flow of information in a single direction, thus making communication in the opposite direction unfeasible. In this way and as necessary, information can be transferred from one network to another more protected one without being able to exploit that connection for information leakage from the protected network, or, on the contrary, allow the sending of information from the protected network without opening an access channel from the outside.

4.3.4.8. CATEGORY: VIRTUAL PRIVATE NETWORKS

60. Intended for the encryption of communication channels, between sender and receiver, through which information in transit is exchanged in order to preserve its confidentiality and integrity. It ranges from hardware devices with the capability of encrypting communications to software applications for the establishment of virtual private networks (VPNs), allowing to create a secure connection with another network over the Internet by creating encrypted tunnels.

4.3.4.9. CATEGORY: VOICE AND VIDEO OVER IP (VVOIP) TOOLS

61. They provide organizations with services that allow two or more people to be connected in real time from different locations, through the network, using a mobile device, computer or *tablet*. They allow audio and video calls between two (2) or more devices, protecting the confidentiality of communications between both ends.

4.3.4.10. CATEGORY: INSTANT MESSAGING (IM) TOOLS

62. They provide organizations with services that allow two or more people to be connected in real time from different locations, through the network, using a mobile device, computer or *tablet*. They allow the sending of text messages and files in real time, between two (2) or more devices, protecting the confidentiality of communications between both ends.

4.3.4.11. CATEGORY: VIDEOCONFERENCING TOOLS

63. The products associated with the category of videoconferencing tools provide organizations with services that allow two or more people to be connected in real time from different locations, through the network, using a mobile device, computer or *tablet*. They allow the establishment of real-time audio and video communication between two (2) or more devices. They have options to share the screen, to make presentations, send documents, schedule meetings and send calls.

4.3.4.12. CATEGORY: WEB APPLICATION FIREWALL (WAF)

64. They analyze and filter traffic to specific web applications. Protection takes place within layer 7 of the OSI model (application layer). They are a specialized type of firewalls or firewalls that are installed in front of web servers, to protect web applications against internal and external attacks.

4.3.4.13. CATEGORY: *SOFTWARE* DEFINED NETWORKS (SDN)

65. *Software-Defined Networking* (SDN) technology allows centralizing the logic associated with controlling communications networks, developing applications to program such networks, and automating network operating processes. In SDN, the *forwarding or data plane* is physically separated from the *control plane*. This differs from traditional networks, where both planes coexist in the same network element

4.3.5. PROTECTION OF INFORMATION AND INFORMATION MEDIA

66. It encompasses the categories of products whose purpose is to strengthen the measures of protection of information, as well as those media on which it is handled, in order to ensure any (or all) security dimensions including its availability, integrity and confidentiality, as well as the non-repudiation of information.

4.3.5.1. CATEGORY: ENCRYPTED DATA STORAGE

67. Intended for the encryption and decryption of all types of data files, as well as storage media such as hard drives or removable memories, in order to protect their confidentiality and to enable only authorized users access to the information contained.

4.3.5.2. CATEGORY: ENCRYPTION AND SECURE SHARING OF INFORMATION

68. Encryption and secure information sharing tools are products that allow you to securely exchange information or files.

4.3.5.3. CATEGORY: SECURE ERASE TOOLS

69. They allow you to delete information in electronic format (files, folders, logical drives, etc.) safely, that is, in a way that the deleted contents are irrecoverable later.

4.3.5.4. CATEGORY: DATA LEAK PREVENTION SYSTEMS

70. Content control products, generally known as *Data Loss/Leak Prevention* (DLP), are those that prevent and prevent unauthorized data transfer and the leakage of information with a high level of confidentiality. They can control physical access to ports and other removable devices to prevent information theft, as well as manage access to information based on user roles and profiles.

4.3.5.5. CATEGORY: TOOLS FOR ELECTRONIC SIGNATURE

71. They include devices and tools that are part of an electronic signature system. By combining these elements, the generation and validation of signatures through digital mechanisms is allowed, allowing, depending on the context, to safeguard the confidentiality, integrity, and non-repudiation of the signed information.

72. The comments will indicate those products that comply with EU Regulation 910/2014 (eIDAS) for qualified electronic signature creation devices.

4.3.5.6. CATEGORY: *HARDWARE SECURITY MODULE* (HSM)

73. This category encompasses *hardware*-based cryptographic devices that generate, store and protect cryptographic keys and often provide *hardware* acceleration for cryptographic operations.

4.3.5.7. CATEGORY: METADATA MANAGEMENT

74. It includes the tools that manage metadata containing files, such as office documents or multimedia files (image, audio, video), in accordance with the metadata treatment policy established in an agency.

4.3.6. PROTECTION OF EQUIPMENT AND SERVICES

75. ICT security lies largely in the proper protection of the equipment on which the information is processed, as well as the services that run on it. It covers product categories that provide a level of security at the platform level, and sometimes also provide cross-sectional security with other security measures than those covered by this taxonomy, as well as protection mechanisms for specific ICT services.

4.3.6.1. CATEGORY: MOBILE DEVICES

76. They include hardware devices, equipped with system software, that facilitate connectivity to mobile networks facilitating mechanisms to establish voice and data communications by different means with other networks or mobile devices.

4.3.6.2. CATEGORY: OPERATING SYSTEMS

77. They compose the basic software used on hardware platforms (computers, mobile phones, tablets, etc.) for the management of machine resources, the management of hardware resources and the provision of services to software application programs.

4.3.6.3. CATEGORY: EMAIL PROTECTION

78. They analyze the flow of emails to prevent those considered harmful from reaching end users. These tools analyze the content of messages for suspicious words and patterns that indicate that they must be filtered or tagged in order not to be forwarded to the mail inbox.

4.3.6.4. CATEGORY: SMART CARDS

79. They allow the execution of programmed logic in their integrated circuits for a wide variety of purposes, while providing interfaces for communication with the systems with which they must interact. In addition, smart cards can be equipped with different protection mechanisms to safeguard the data they contain or the data exchanged to carry out the functionality they are intended for.

4.3.6.5. CATEGORY: BACKUPS

80. They allow to enforce backup policies defined by the organization. These tools allow you to make backups of storage systems, equipment or entire systems.

4.3.6.6. CATEGORY: RELIABLE PLATFORMS

81. Products or systems that serve as a basis or support for the execution of certain software modules.

4.3.6.7. CATEGORY: VIRTUALIZATION

82. The products associated with the virtualization category are mainly oriented to take advantage of the same hardware infrastructure that will be shared with multiple isolated environments each with its own operating system, enabling the improvement in the efficiency and flexibility of ICT resources. The **hypervisor, or Virtual Machine Manager (VMM[10])**, is the component of the product that allows physical equipment to support the various virtual environments with their configurations. Each virtual environment is encapsulated in **a virtual machine (VM[11])** that has virtual resources allocated, such as memory, processor, guest operating system, and applications.

4.3.6.8. CATEGORY: LOAD BALANCERS

83. The products associated with the category of Load Balancers or Application Delivery Controllers are aimed at controlling the bandwidth between different elements of

[10] *Virtual Machine Management*
[11] *Virtual Machine*

the system, mainly between client computers (internal or external) that make requests to servers that serve them. Balancers are *software* or *hardware* products that aim to avoid saturation of services, optimizing the allocation of resources between different independent or clustered servers.

4.3.6.9. CATEGORY: CASB

84. CASB (*Cloud Access Security Broker*) products respond to the need for visibility and control over the use of an organization of cloud applications and services. They represent a central point where the organization can implement security policies that regulate the use of applications and cloud services by users and devices.

4.3.6.10. CATEGORY: HYPERCONVERGENCE

85. Hyperconverged Infrastructure (HCI) is a *software*-based architecture approach that provides storage, compute and networking resources transparently to the *hardware* being used, with large horizontal scaling capabilities and all managed from a single centralized point. The products associated with this category integrate compute, storage and network capabilities into one operating layer and centralize all data center management tasks, at the *software* level.

4.3.6.11. CATEGORY: VIDEOIDENTIFICATION TOOLS

86. The products associated with this category arise to respond to the need to establish mechanisms of authentication and remote identification, in order to contribute to the reduction of the movement of citizens to carry out procedures, without diminishing their rights. These tools make comparisons between a person and their ID photo and implement real-time security controls, such as the detection of holograms, badges, patterns, and other identity document security elements.

4.3.6.12. CATEGORY: VIRTUAL DESKTOP INFRASTRUCTURE (VDI)

87. VDI is a technology that allows users to have a desktop environment, accessible remotely through a client device. The user can manage an entire desktop or an application, in the same way as if it was running on its own. VDI provides flexibility and efficiency to organizations when it comes to managing IT resources. It also gives employees facilities in developing their work, regardless of their physical location.

4.3.6.13. CATEGORY: KVM SWITCHES

88. KVM (Keyboard-Video-Mouse) switches are hardware devices that allow the user to control multiple computers from one or more sets of keyboards, video monitors and mice. They allow you to select which computer you want to activate, thus showing its video output and being controlled by the keyboard and mouse.

4.3.6.14. CATEGORY: DATABASE MANAGEMENT SYSTEMS (DBMS)

89. Database Management Systems (DBMS) facilitate the use and manipulation of databases in a safe, simple and orderly way. It provides users with a systematic way

to create, retrieve, update and manage data, ensuring that data is consistently organized and remains easily accessible.

4.3.7. PROTECTION OF INSTALLATIONS AND INFRASTRUCTURES

90. It includes categories of products and services whose purpose is to strengthen the protection measures of facilities and infrastructures.

4.3.7.1. CATEGORY: IP CAMERAS

91. The products belonging to this category allow video and audio capture and transmission securely digitally, whether for viewing, local or remote storage, or processing in a video management tool.

4.3.7.2. CATEGORY: VIDEO MANAGEMENT

92. The products belonging to this category allow the visualization, storage, management and analysis of events and the sending of alerts from one or more sources of video capture. They also allow centralized management of the video surveillance system.

4.3.8. SAFETY OT

93. It includes specialized tools to protect Operations Technology (OT) systems, used in industrial environments or critical infrastructure.

4.3.8.1. CATEGORY: ELECTRIC VEHICLE CHARGING STATIONS

94. The products belonging to this category allow the rapid recharging of the batteries of electric vehicles through direct connection to the electrical grid.

4.3.9. CLOUD SECURITY SERVICES

95. Includes *cloud* services that provide security features. Such security functionality must be associated with one of the categories included in the taxonomy detailed in this document.

4.3.10. OTHER TOOLS

96. It collects tools whose main security functionality does not fall within any other of those published.

4.3.11. TOOLS FOR THE DEVELOPMENT OF SAFETY PRODUCTS

97. It includes those *software* and firmware components that have been evaluated by the National Cryptologic Center for the development of security products.

98. Since components of various kinds appear in this classification, no annex to this guide will be created containing the fundamental safety requirements associated with it.

5. TAXONOMY OF APPROVED PRODUCTS

99. The taxonomy of products approved for handling classified information shall be the same as for qualified products together with categories detailed in the following sections.

100. The Fundamental Safety Requirements (RFS) shall be the same as those set out in this Guide for Qualified Products, updated with the specific cryptographic mechanisms described in Annex H. In addition, a TEMPEST evaluation and/or a cryptological evaluation of the product may be required as the case may be.

101. In case a cryptological evaluation of the product is necessary, the requirements set out in the CCN-STIC-130 Guideline "Requirements for Cryptological Assessment" should be considered. [3]. The detailed ICT Security Product Approval Procedure is included in the CCN-STIC-102 Guidance Procedure for Approval of ICT Security Products to Handle National Classified Information [2].

5.1 CATEGORY: PROTECTION IN TACTICAL ENVIRONMENTS

102. This category includes product categories whose main purpose is the protection of information and communications in tactical or deployed environments.

103. This category also includes a specific category that identifies different information systems for use in tactical environments that, under certain configuration conditions, and always using products from the other categories in this category, are approved to process national classified information up to a certain level. This approval does not exempt from the procedure for the accreditation of systems handling classified information, as defined in Guideline CCN-STIC-101 Accreditation of ICT Systems Handling Classified Information [5]the adoption of a tactical information system is only intended to facilitate the system's own accreditation.

104. Communications in tactical or deployed environments have certain particularities that differ markedly from communications through fixed networks and infrastructures. These include:

- The time during which information is relevant is usually shorter than in other environments. For example, the position of a military unit generally only matters for the period of time that the unit is in a given location.
- The impact associated with compromising information confidentiality may include other associated damages that go beyond the criticality of the information itself. Following the example above, the position of a military unit may not have a very high ranking level, but its commitment may put human lives at risk.
- The networks used are generally deployable and proprietary, although in certain specific situations network infrastructures belonging to public operators can also be used.
- Proprietary networks are generally not connected to the Internet.

- The transmission media used are generally wireless such as military radios, digital *trunking* equipment (TETRA, TETRAPOL…), *Wi-Fi* and LTE equipment, etc. These means of transmission are often *half-duplex* in nature , they have a low bandwidth, an error rate that can be high, there is no guarantee of connectivity, etc. Therefore, it is not feasible to employ certain encryption solutions commonly used in fixed network infrastructures (e.g. classic IP encryptors with session key negotiation), and it is necessary to employ specific encryption solutions adapted to the means of transmission used.
- Certain characteristics of tactical deployments may sometimes allow assuming that the threat level for certain short-range transmission media is lower than in other environments. These include the establishment of security and surveillance perimeters (e.g. at command posts), the short stay of a mobile node in the same location, etc.
- In this type of products, plus allah of the COMSEC mechanisms, other aspects such as the TRANSEC and NETSEC mechanisms are also of special importance.

105. Given the multiplicity of possible tactical scenarios, the limitations on the use of products belonging to the categories of this category will be perfectly defined in the corresponding procedure for the use of the product.

5.1.1. CATEGORY: RELIABLE TACTICAL PLATFORMS AND DEVICES

106. Platforms and devices for tactical environments that are considered as a secure container for running software applications in a secure manner (e.g. command and control applications).

107. In general, the same Fundamental Security Requirements applicable to the Trusted Platforms category will apply.

108. This category does not provide for the protection of information in transit, the encryption of which must be performed by a solution for the protection of tactical communications (e.g., an encryption application that runs on the platform itself or trusted tactical device). Therefore, approvals of these platforms and devices in isolation will only be valid for the processing of locally classified information, but not for the transmission of it over unsecured networks.

5.1.2. CATEGORY: SOLUTIONS TO PROTECT TACTICAL COMMUNICATIONS

109. They allow the protection of communications in tactical environments in one or more security dimensions (confidentiality, integrity, authenticity, availability and/or traceability), adapting to the particularities of the means of transmission used.

110. It will include different types of products suitable for different classification levels that will be explicitly indicated: Tactical encryptors, military radios, encryption software applications, etc.

111. In the case of encryption *software* applications, they must be run on platforms or tactical devices that are considered reliable and belong to the previous category (they will be identified in the secure use procedure of the encryption application).

112. In the case of military radios, taking into account their reconfigurable nature, the approval of each of them will unequivocally identify the waveforms and sets of COMSEC, NETSEC and TRANSEC algorithms included in that approval. Only those waveforms whose COMSEC mechanisms have been approved after passing the corresponding cryptological assessment shall be included.

113. This category will also specify the approval of certain products belonging to other categories for use in tactical environments, allowing their use to protect classified information of a higher degree of classification than that contained in its general approval (e.g., see CCN-STIC-497 on the use of Wi-Fi on classified networks). The conditions under which the approval of an existing product is specified shall be defined in an exclusive and dedicated use procedure for those conditions of use.

5.1.3. CATEGORY: INFORMATION SYSTEMS FOR TACTICAL ENVIRONMENTS

114. Information systems for use in tactical environments, such as command and control systems, using approved products belonging to the previous categories of this category and approved for processing national classified information.

115. To include an information system in this category, the degree of compliance with the STIC requirements contained in CCN-STIC-301 STIC requirements will also be checked [6].

6. TAXONOMY OF PRODUCTS AND SERVICES OF COMPLIANCE AND SECURITY GOVERNANCE

116. Table 3 shows the scheme of the taxonomy of **products of conformity and governance of safety**, as well as the list of annexes to this document, where the requirements for each of the categories that make up this taxonomy are collected.

CATEGORY	ANNEXES
Governance and Security Planning	CG.1
Safety and Compliance Regulations	CG.2
Risk Analysis and Management	CG.3
Notification and Management of Cyber Incidents	CG.4
Exchange of Cyberintelligence	CG.5
Training And awareness in Cybersecurity	CG.6

Table 3. Taxonomy of Compliance Products and Security Governance

6.1 CATEGORY: GOVERNANCE AND SECURITY PLANNING

117. To this category belong those solutions that offer assistance to users in obtaining information about the security status of the systems of the organizations, based on a measurement standard, providing indexes that allow to evaluate the data obtained, interpret them and make strategic decisions. They could also facilitate the development of adequacy plans and the achievement of the corresponding set of technical measures to be applied to systems based on a pre-established category.

6.2 CATEGORY: SAFETY AND COMPLIANCE REGULATIONS

118. This category consists of solutions that assist users in the execution of audit preparation tasks, compliance and certification management, and system security management as a whole. In addition, it offers assistants oriented to support auditors and audit bodies, through audit evidence gathering capabilities, audit checklists and notebooks, reporting generation and any other task required in the different phases of the audit.

6.3 CATEGORY: RISK ANALYSIS AND MANAGEMENT

119. To this category belong those solutions that offer assistance to users in the elaboration of risk analysis associated with the systems, based on an established standard, by identifying the threats to which the essential assets of the system are subjected and analyzing the likelihood and impact of their materialization. They will also offer the possibility of mitigating or reducing the associated risks through safeguards.

6.4 CATEGORY: NOTIFICATION AND MANAGEMENT OF CYBER INCIDENTS

120. To this category belong those solutions that automate processes, classify incidents, facilitate the monitoring of their management and allow coordination between the different actors involved. They can provide assistance to operators who manage incidents or users who report security incidents to a central body or entity.

6.5 CATEGORY: CYBERINTELLIGENCE EXCHANGE

121. To this category belong those solutions for the management and exchange of cyberintelligence, providing means to improve the capabilities of prevention, analysis and detection of cyberthreats.

6.6 CATEGORY: TRAINING AND AWARENESS IN CYBERSECURITY

122. This category includes solutions dedicated to evaluating, training, reinforcing and/or measuring the levels of training and awareness in cybersecurity of the employees of an organization.

7. REFERENCES

[1] CCN-STIC-105 ICT Security Product Catalog (CPSTIC).

[2] CCN-STIC-102 Procedure for Approval of ICT Security Products to Handle National Classified Information.

[3] CCN-STIC-130 Requirements of the cipher products to pass the Cryptological Assessment.

[4] CCN-STIC-151 Evaluation and TEMPEST Classification of Equipment.

[5] CCN-STIC-101 Accreditation of ICT Systems Handling Classified Information.

[6] CCN-STIC-301 STIC REQUIREMENTS.

[7] CCN-STIC-106 Procedure for the inclusion of qualified ICT security products in the CPSTIC.

8. ABBREVIATIONS

CCN	*National Cryptologic Center*
CPSTIC	*Catalog of Information and Communication Technology Security Products*
DLP	*Data Loss/Leak Prevention*
EDR	*Endpoint Detection and Response*
ENS	*National Security Scheme*
PPE	*Endpoint Protection Platform*
HSM	*Hardware Security Module*
IDS	*Intrusion Detection System*
IM	*Identity Management*
IPS	*Intrusion Prevention System*
IPsec	*Internet Protocol Security*
GO	*Incident Response*
MAC	*Media Access Control*
NA	Not applicable
NAC	*Network Access Control*
NGEPP	*Next Generation Endpoint Protection Platform*
OSI	*Open Systems Interconection*
PAM	*Privileged Access Manager*
RD.	Royal Decree
RFS	Fundamental Safety Requirements
SIEM	*Security Information and Event Management*
STIC	Security of Information and Communication Technologies
ICT	Information and Communication Technologies
TLS	*Tranport Layer Security*
EMU	*Unified Endpoint Management*
URL	*Uniform Resource Locator*
VM	*Virtual Machine*
VMM	*Virtual Machine Manager*
VPN	*Virtual Private Network*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL