National Cryptologic Centre

Training Offer 2022

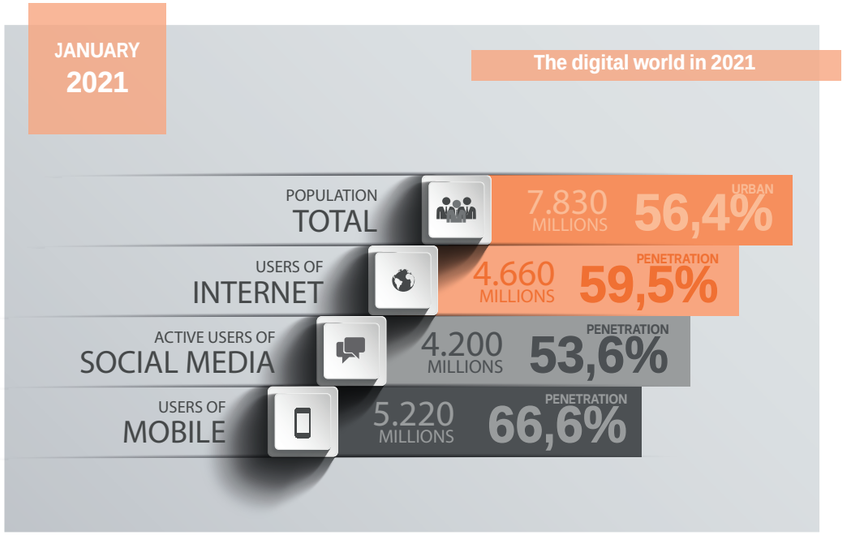
ángeles

Formación, capacitación y talento en ciberseguridad

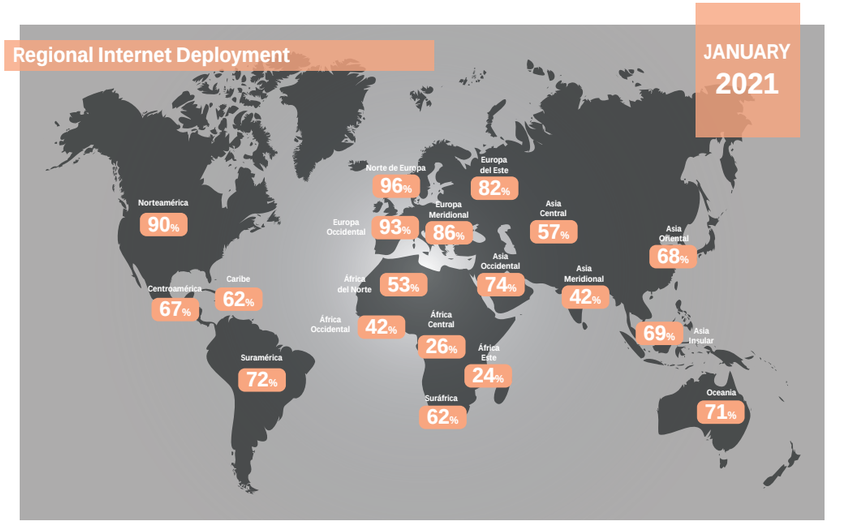
Index

1. Training needs and new challenges

The evolution of new technologies, especially those related to information and communication, and the widespread use of the Internet, has led to the development of a new scenario: cyberspace, whose protection against possible threats and aggressions is essential.



Source: Digital 2021 Global Overview Report (We Are Social)



Source: Digital 2021 Global Overview Report (We Are Social)

To achieve a secure cyberspace, where risks can be mitigated to a manageable extent, it is essential to raise awareness and sensitise society; only through continuous training can cybersecurity incidents be prevented and dealt with in a timely manner.

Faced with the need to promote and develop qualified professional profiles for the public sector, **The National Cryptologic Centre (CCN)** has developed the **Ángeles platform** for cybersecurity training and culture. Here you can find all the resources developed by the CCN, both in terms of training and awareness-raising and sensitisation on the subject.

Ángeles brings together cybersecurity training courses, both face-to-face and online, adapted to the user's profile and level of training. These courses are structured in this **Training Offer**, which has been transformed as technologies have evolved, adapting to the new scenario presented by cyberspace.

The training offered by the National Cryptologic Centre has been designed to provide an effective response to the challenges of the 21st century. In view of the need for this response to be comprehensive, the CCN makes available to the public sector, the private sector, the media and even from other states, their knowledge and experience in training .

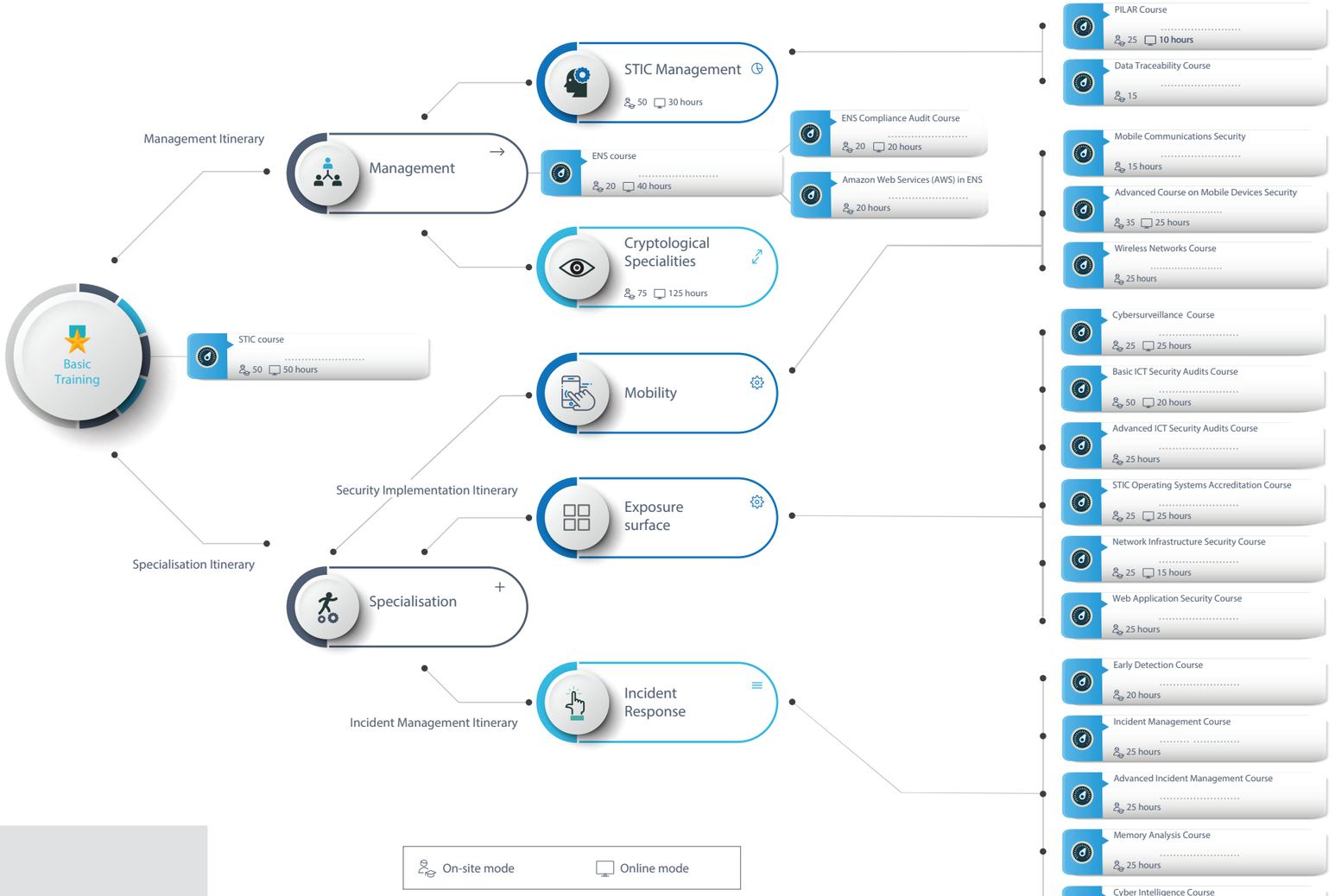
In addition, as a guarantee of successful completion of the training, the CCN awards those participants who have passed the course with flying colours a **Certificate** specifying the subjects and associated credits.

2. Curricular training

The Training Offer of the National Cryptologic Centre has been designed in response to the need for training, both face-to-face and on-site to qualified professionals with different profiles and level of training. For this reason, a **BASIC training** has been established which, through the STIC course, introduces the student to the field of Information and Communication Technologies Security.

Once the basic training has been completed, the professional who wishes to improve the training can choose two pathways: **management** and **specialisation**. The first, in turn, has two branches: STIC management and the **Cryptologic Specialities** branch.

The specialisation pathway, aimed at more technical personnel, includes the **Audit** module and the **Incident Management** module, each comprising a set of courses that allow the student to specialise in the subject.



Purpose

The aim of the **"Information and Communications Technology Security Course"** is to provide attendees with the necessary knowledge to achieve an adequate awareness of ICT systems security and the threats and vulnerabilities posed by new technologies.

Credits / Syllabus Hours

The distribution of the 50 hours of the asynchronous phase of the course (5 credits) is as follows:

- Theory: 5 credits / 50 hours

The distribution of the 50 hours of the synchronous phase of the course (5 credits) is as follows:

- Theory: 4.5 credits / 45 hours
- Practical: 0.5 credits / 5 hours

Standards and Certificate of Achievement

As this course is held in two phases (asynchronous and synchronous), in order to participate in the synchronous phase, it is essential to pass the tests corresponding to the exams scheduled during the asynchronous phase, in which the knowledge acquired in this phase is assessed.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Public employees in subgroups A1, A2, B and C1, and the equivalent employment staff, who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with the security of the same, may apply for the course.

Priority for the selection of participants to the course will be considered to be developing, in their current assignment, activities of planning, management or administration of ICT Systems, or its Security, for a period of more than one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. The learner must take into account the following requirements:

- The email account used for communication between the tutor and the students can be a personal or work email account, but it must match the one indicated in the online application form.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Basic Cybersecurity Course (Distance Learning Phase)	- Introduction to cybersecurity. - Threats. - Security policies.	2,0	2,0	0	Introduction. Types of threats. The Deep Web. Applications. Secure browsing and e-mail. Virtualisation. Security in mobile devices and wireless networks. Instant messaging and social networking. IoT. Security Policy.
Course on Security of Information and Communication Technologies (Distance Learning Phase)	- Introduction to STIC. - Security Regulations. - Security Policies. Accreditation Procedure. - STIC inspections. - Incident Management. Security Tools. - Perimeter Security. - Wireless Networks.	3,0	3,0	0	Security Guidance. STIC Concepts and Terminology. Introduction to Cryptology. Cryptosystems and Modes of Use of the Cipher. Introduction to Cryptophony. Security Organisation and Management. ICT Security Policy. Systems Accreditation. Vulnerabilities, Threats and Risks. Security Documentation. STIC Inspection. TEMPEST and TRANSEC threat. Security Incident Management. Malicious Software. Security Tools. Perimeter security. Systems interconnection. Firewalls and Intrusion Detection Systems. Wireless Security.
Introduction: Approach to cybersecurity	- Approach to cybersecurity. - ENS-RGPD.	0,4	0,4	0	Spanish approach to cybersecurity. ENS: update, status, modifications. ENS-RGPD.
ENS: Validation Environment, Adequacy Plan	- ENS: Validation environment. Suitability plan. - Risk Analysis.	0,3	0,2	0,1	ENS Validation Environment (EVENS). Adequacy Plan. Risk Analysis. Declaration of Applicability. Case studies.
Cryptologic Security	- Cryptologic Coordination. Cryptologic Security.	0,2	0,2	0	Cryptologic Coordination. Cryptologic Security. STIC equipment.
STIC Policies	- Introduction to STIC. - Security Regulations. - Security policies.	0,4	0,4	0	Cybersecurity strategies. National legislation. National IT Security Evaluation and Certification Scheme. IT Security Evaluation Criteria. ICT Security Policy in the Administration. ICT Security Organisation.

STIC procedures	- Accreditation Procedure. - Risk Analysis and Management. - STIC inspections. - Incident Management. - TEMPEST threat.	1,3	1,1	0,2	Risk Analysis and Management. MAGERIT and PILAR Tool. Physical, Documentary and Personnel Security. Compliance profiles. Exposure area environment. Continuous safety assessment. STIC Inspection Procedure. System Interconnection. Incident Management. Threat TEMPEST.
STIC Technical Measures	- Security Tools. - STIC equipment.	2,0	2,0	0	Audit solutions. Wireless security. Harmful code analysis. Web security. Cybersurveillance. Endpoint Security. Mobile Security.
Miscellaneous Group	- Inauguration and Closing.	0,4	0,2	0,2	Examination. Inauguration. Critical Assessment and Closing.

Mode: Online tutored

- Asynchronous phase: 50h.
- Synchronous phase: 50h

Purpose

The aim of the **"National Security Scheme (ENS) Course"** is to provide attendees with the necessary knowledge to implement the ENS (Spanish initials) and its contribution to mitigate current threats.

- Acquire the knowledge and become familiar with the activities necessary to carry out the ENS Compliance Plan in an organisation; deepen the roles and committees necessary for proper governance based on an assessment of essential assets and the categorisation of the information systems that support them.
- Implementation of the ENS, starting from a previous Adaptation Plan; understanding each of the ENS security measures according to the category of the system and how they should be implemented; as well as understanding the importance of outsourcing in the public sector.
- Understand the essential concepts of audits and be familiar with the ENS Certification Scheme and the different tools that the CCN makes available to organisations to facilitate compliance with the ENS.

Credits / Syllabus Hours

The distribution of the 40 hours of the asynchronous phase of the course (4 credits) is as follows:

- Theory: 2.8 credits / 28 hours
- Practical: 1.2 credits / 12 hours

The distribution of the 20 hours of the synchronous phase of the course (2 credits) is as follows:

- Theory: 1.6 credits / 16 hours
- Practical: 0.4 credits / 4 hours

Standards and Certificate of Achievement

As this course is held in two phases (asynchronous and synchronous), in order to participate in the synchronous phase, it is essential to pass the tests corresponding to the exams scheduled during the asynchronous phase, in which the knowledge acquired in this phase is assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the four (4) days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade for the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase that starts later.

Any modification of the above, due to circumstances requiring it, will be reflected in the course completion report.

Addressees

Public employees of subgroups A1, A2, B and C1, and equivalent labor personnel, who have responsibilities in the planning, management, administration or security of information and communications technology systems and who, Likewise, you need for your job to carry out tasks related to the adaptation to the National Security Scheme of your organization.

Priority for the selection of participants for the course will be given to those who are carrying out, in their current assignment, activities of planning, management or administration of ICT Systems, or the Security thereof, for a period exceeding one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the learner must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. The learner must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Brief Description of Content	- Introduction to the ENS. - ENS Compliance Plan. - Implementation of Security Measures (I and II). - Public Sector Procurement. - ENS - ISO comparisons 27001. - Audits and Certification in the ENS.	4,0	2,8	1,2	Introduction to the ENS. Legal and policy justification. E-administration and security. Phases of compliance. Risk management. Structure of a Management System. Adequacy Plan. Introduction to Annex II. Maturity levels. Organisational Framework. Operational framework. Protective measures. Compensatory measures. Suppliers. Supply chain. On-Premise solutions. Procurement in the Public Sector. ENS - ISO 27001. ENS Certification. Monitoring and improvement of an ISMS. Audits.
National Security Scheme	- General concepts. Legal framework. Phases of compliance. - Adequacy plan. - Roles and responsibilities. - Categorisation of systems. Risk management. - Implementation of the ENS. Security measures. - Supply chain. - Audits and Compliance. - CCN tools.	1,8	1,4	0,4	Introduction to ENS: current status, basic principles and minimum requirements, managed security. Assets and critical assets. Scope of application. Legal framework and regulations: difference between legal norms and standards. Security ITS. ENS compliance phases: Deming Cycle and its phases. Compliance plan. Implementation of the plan. Continuous improvement. Committees, roles and responsibilities. Policy Information Security. Identification and valuation of essential assets. Valuation and categorisation of systems: security dimensions, valuation levels, valuation criteria. Dependencies between assets. Risk Analysis and Management, MAGERIT methodology, PILAR tool. Implementation of the ENS and the security improvement plan. ENS security measures and compliance profiles. The supply chain and outsourcing in the public sector: harmonisation of security measures. Audits and evidence ENS compliance: introduction, technical and management audits. Declaration and Certification of compliance. Certification process. The Corrective Action Plan (CAP). CCN tools to facilitate the compliance with the ENS.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Assessment and Closing.

Mode: Online tutored

- Asynchronous phase: 40h.
- Synchronous phase: 20h.

Purpose

The purpose of the **"ENS Compliance Audits Course"** is to provide attendees with the knowledge and skills necessary to carry out ENS Certification Audits, in accordance with the Resolution of 27 March 2018 of the Secretary of State for Public Service, which approves the Technical Security Instruction on Information Systems Security Audits, in all phases of the audit process: preliminary documentary study, remote/in situ audit and drafting of the Audit Report.

Credits / Syllabus Hours

The distribution of the 20 hours of the asynchronous phase of the course (2 credits) is as follows:

- Theory: 2 credits / 20 hours

The distribution of the 20 hours of the synchronous phase of the course (2 credits) is as follows:

- Theory: 0.5 credits / 5 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

As this course is developed in two (2) phases (asynchronous and synchronous), it will be an essential condition to participate in the synchronous phase, to pass the tests corresponding to the exams scheduled during the asynchronous phase in which the knowledge acquired in this phase will be assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the four (4) days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Public employees of subgroups A1, A2, B and C1, and the equivalent employment staff, who have responsibilities in the planning, management, administration or security of information and communication technology systems and who also need to carry out tasks related to the compliance of their organisation with the National Security Scheme, may apply for the course.

Priority for the selection of participants to the course will be considered to be developing, in their current assignment, activities of planning, management or administration of ICT Systems, or the Security of the same, for a period of more than one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado. ccn-cert.cni.es/), where the e-learning platform is located. The learner must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Course on ENS Audits (Asynchronous e-learning phase)	- Information Systems Audits. - General concepts of ENS Audit and Certification. Development and execution of an audit.	2,0	2,0	0	Definition of audit. Audit criteria. Preliminary definitions. Essential principles. Audit programme. Implementation. Definition of objectives, scope and criteria. Results management. Scope. Technical competence. Resources of the Certification Body. Audit time. Audit findings. Remote certification. Shared services. Conformity mark. Certification in exceptional situations. Obligations of the Entities. Provisional approval of conformity. Scope and purpose. Audit team. Planning. Evidence. Preparation and presentation of findings. Presentation of the report. Final opinion.
STIC Technical Measures	- ENS compliance audits. Audit Methodology. - Audit Plan. - Evaluation of the Adequacy Plan. Implementation Assessment. Audit report. Corrective Action Plan	1,8	0,3	1,5	Introduction. Basic concepts and process of compliance with the ENS. Planning the audit process. Assessment of the Adequacy Plan: categorisation, statement of applicability and security policy. Risk analysis. Implementation assessment: operational framework, protection measures. Audit report and corrective action plan. Minimum requirements and composition of OAT. CCN-CERT Solutions (INES-AMPARO-PILAR)
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Assessment and Closing.

Purpose

The purpose of the **"STIC Course - Amazon Web Services (AWS) in the ENS"** is to provide attendees with the necessary knowledge to understand and define the necessary measures and configurations in public cloud environments in Amazon Web Services (AWS) for the correct application of the requirements of the National Security Scheme.

The programme takes the format of a self-contained course with the purpose of providing attendees with a practical overview of the knowledge and operation of AWS environments with a focus on security-oriented Amazon Web Services.

In that context, the course has been designed to combine methodology with technology within a process of deploying and operating cloud environments. Much of the content is dedicated to introducing AWS and its core services so that even trainees with no previous AWS experience can understand the basics of AWS.

Credits / Syllabus Hours

The distribution of the 20 hours of the synchronous phase of the course (2 credits) is as follows:

- Theory: 1.5 credits / 15 hours
- Practical: 0.5 credits / 5 hours

Standards and Certificate of Achievement

As this course is carried out in synchronous mode, attendance or connection to all the scheduled sessions will be compulsory, as well as a series of practical exercises that will make it possible to assess whether the appropriate knowledge has been obtained in order to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be withdrawn from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2, B and C1, and equivalent employment staff, who have responsibilities in the planning, management, administration or security of information and communications technology systems and who also need to carry out security tasks and regulatory compliance with the National Security Scheme for their job, may apply for the course.

Attendees are expected to have a minimum knowledge of communications and security. Optimal use of the training will be achieved if there is also previous knowledge or experience with the National Security Scheme and public cloud environments.

Priority for the selection of participants to the course will be considered to be developing, in their current assignment, activities of planning, management or administration of ICT Systems, or the Security of the same, for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Amazon Web Services (AWS) in the ENS	- Introduction to ENS. - Introduction to AWS - Configuration guides safe. - Security controls. - Protection of Information and Services.	1,8	1,3	0,5	Introduction to ENS. Shared responsibility model. Introduction to AWS. Secure configuration guidelines. Prowler Lab. Security in the AWS Cloud. AWS IAM. Amazon EC2. Amazon VPC. Containers on AWS. Serverless and AWS Lambda. Storage on AWS. Databases on AWS. Encryption on AWS. Monitoring of resources in AWS. Exploitation - Inventory and key protection. KMS and ENS. Security controls in AWS. Threat and vulnerability detection. Information protection. Protection of services.
Miscellaneous Group	- Inauguration and Closing	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Mode: Online tutored

- Synchronous phase: 20 h

Purpose

The aim of the **"Course on Security Management of Information and Communication Technologies and the National Security Scheme (STIC Management)"** is to:

- Provide the necessary knowledge for the analysis and risk management of an ICT system. As a result, they will be able to draft and implement appropriate security procedures and policies to protect the information processed, stored or transmitted by a system.
- To familiarise participants with the use of the PILAR tool (Procedure for Computerised and Logical Risk Analysis) and to be able to carry out a formal risk analysis following the MAGERIT methodology.
- To provide the knowledge and skills necessary to be able to decide which technologies, strategies and tools are necessary in each specific organisation to verify the security of networks, applications and devices as well as to verify and correct processes and implementations.
- Provide the necessary support to be able to implement the measures proposed in the **National Security Scheme (ENS)**.

Credits / Syllabus Hours

The distribution of the 30 hours of the asynchronous phase of the course (3 credits) is as follows:

- Theory: 3 credits / 30 hours

The distribution of the 50 hours of the synchronous phase of the course (5 credits) is as follows:

- Theory: 3 credits / 30 hours
- Practical: 2 credits / 20 hours

Standards and Certificate of Achievement

As this course is held in two phases (asynchronous and synchronous), in order to participate in the synchronous phase, it is essential to pass the tests corresponding to the exams scheduled during the asynchronous phase, in which the knowledge acquired in this phase is assessed.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of public administrations in groups A1 or A2 who have responsibilities at management level, or in the planning, management or administration of information and communications technology (ICT) systems, or with their security, may apply for this course.

The following are considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at managerial or technical level, in the implementation or operation of ICT Systems or in the management of the Security of such Systems for a period of more than one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. In the registration process, a username and password are established for connection to the Portal. Before the course is held, students will be provided with the details and instructions for accessing the asynchronous phase by e-mail. The student will have to take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Policies	- Introduction to STIC. - Security Regulations. - Security policies.	0,6	0,6	0	Security Guidance. STIC Concepts and Terminology. Introduction to Cryptology. Cryptosystems and Modes of Use of the Cipher. Introduction to Cryptophony. Organisation and Security Management.
STIC procedures	- Accreditation Procedure. - STIC inspections. - Incident Management.	0,5	0,5	0	Systems Accreditation. Vulnerabilities, Threats and Risks. Security Documentation. STIC Inspection. TEMPEST and TRANSEC threat. Security Incident Management.
STIC Technical Measures	- Security Tools. - Perimeter Security. - Wireless Networks.	0,5	0,5	0	Malicious Software. Security tools. Perimeter security. System Interconnection. Firewalls and Intrusion Detection Systems. Wireless Security.
National Security Scheme	- Introduction and Categorisation of the ENS - Security Auditing and Organisation in the ENS - Evaluation and Certification.	2,8	2,8	0	National Security Scheme. Audit and Accreditation Procedure. Security Organisation. Security Documentation. Security Incident Management.
Risk Analysis and Management	- Risk Analysis and Management. - MAGERIT methodology. - PILAR tool.	2,2	1	1,2	Introduction to Risk Analysis and Management. Assets. Threats, Impact and Risk. PILAR Tool Installation. Safeguards and Assessments. Generation of Security Documentation. Practical examples.
STIC Inspections	- Interconnection in the ENS - STIC inspections. - Security in Web and Wireless Environments	0,8	0,8	0	Introduction to STIC Inspections. Security Tools and Checks. Security in Systems and Devices. Security in Web Applications. The Human Factor. Case studies.
Miscellaneous Group	- Inauguration and Closing..	0,6	0,6	0	Preliminary Examination. Inauguration. Critical

Purpose

The purpose of the **"STIC Course - PILAR Tool"** is to provide the necessary knowledge and skills to be able to assess the security status of a system, identifying and assessing its assets and identifying and assessing the threats to them.

To familiarise participants with the use of the PILAR (Procedure for Logical and Computerised Risk Analysis) tool by being able to carry out a formal risk analysis following the MAGERIT methodology.

Credits / Syllabus Hours

The distribution of the 10 hours of the asynchronous phase of the course (1 credit) is as follows:

- Theory: 1 credit / 10 hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

As this course is held in two phases (asynchronous and synchronous), in order to participate in the synchronous phase, it is essential to pass the tests corresponding to the exams scheduled during the asynchronous phase, in which the knowledge acquired in this phase is assessed.

During the synchronous phase of the course, participants will have to carry out a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "PASS". If they do not pass the minimum required, the student will be considered "NOT APT" and will be withdrawn from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Personnel in the service of Public Administrations in groups A1, A2 or C1 who have responsibilities at a technical level in the planning, management, administration or maintenance of Information and Communications Technology Systems (ICT), or with their security, may apply for this course. For military personnel, the Ministry of Defence will issue a specific call for applications.

The following are considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- To have previously completed the Information and Communications Technology Security Management Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.

• Have responsibilities, at managerial level, in the implementation or operation of ICT Systems or in the management of the Security of such Systems for a period of more than two (2) years.

Course access (Asynchronous phase)

Each selected student will be provided with the address of the e-learning platform, a username and a password to connect to the course by e-mail. This information will be sent prior to the course so that they can familiarise themselves with the methodology and the platform. The student will have to take into account the following requirements:

• The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.

• The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Risk Analysis and Management (asynchronous phase)	- Risk Analysis. - Introduction to Risk Management.	1	1	0	Risk Analysis (assets, threats, safeguards, impact indicators). Risk Rating.
STIC Technical Measures	- Risk Analysis. - Risk Management. - Treatment of Risks.	2,4	0,8	1,6	Risk Analysis (assets, threats, safeguards, impact indicators). Mythology. Tools. Risk Management Cycles. Master plan. Costing. Underwriting methods. PILAR tool
Miscellaneous Group	- Inauguration and Closing.	0,1	0,1	0	Inauguration. Critical Judgement and Closure.

Purpose

The purpose of the **"STIC Course - Data Traceability"** is to provide attendees with the necessary knowledge to manage the organisation's sensitive and confidential documentation through a data-centric security approach, so that it can be protected and under control in any location, as well as to obtain a complete audit of access to it.

Credits / Syllabus Hours - Fase síncrona

The distribution of the 15 hours of the synchronous phase of the course (1.5 credits) is as follows:

• Theory: 1 credits / 10 hours

• Practical: 0.5 credits / 5 hour

Standards and Certificate of Achievement

As this course is carried out in synchronous mode, attendance at all the scheduled sessions will be compulsory, as well as a series of practical exercises that will make it possible to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be withdrawn from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2, B or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

• To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.

• Have completed courses related to IT or IT security.

• Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Data traceability	- Actors and types of information leakage attacks. - Technologies to prevent information leakage. - Data-centric security systems. - Classification and traceability information. - Zero-Trust and SASE security models. - CARLA tool. - Case studies on data-centric protection and traceability.	1,5	0,9	0,9	Introduction to a data-centric approach to security. Attack vectors on sensitive information and typology of information leaks. The Zero-Trust and SASE security model and its relationship with data-centric security. Use cases and benefits of a data protection, control and traceability solution. CARLA Tool: Data Protection, Control and Traceability. Practical sessions on traceability and control of sensitive documentation
Miscellaneous Group	- Inauguration and Closing.	0,1	0,1	0	Inauguration. Critical Judgement and Closing.

Purpose

The aim of the **"Cryptologic Specialities Course"** is to provide participants with the basic knowledge necessary to:

- the appropriate choice of cryptological techniques and parameters to be used in an encrypted network.

The aim of the **"Cryptologic Specialities Course: Phase II - Cryptologic Equipment"** is to provide participants with the necessary knowledge to administer and manage encryption networks with the appropriate ciphers and regulations.

Credits / Syllabus Hours - Asynchronous Phase

The distribution of the 125 hours of the asynchronous phase of the course (12.5 credits) is as follows:

- Theory: 12.5 credits / 125 hours

Credits / Syllabus Hours - Synchronous Phase

The distribution of the 75 hours of the synchronous phase of the course (7.5 credits) is as follows:

- Theory: 6.7 credits / 67 hours
- Practical: 0.8 credits / 8 hours

Standards and Certificate of Achievement

As the course is held in two phases (asynchronous and synchronous), in order to be appointed as an assistant in the synchronous phase, it is essential to pass the tests corresponding to the preliminary exam in which the knowledge acquired in the asynchronous phase is assessed.

The preliminary exam will consist of answering a total of 30 theoretical test-type questions in written format with four possible answers (only one true answer), with no points deducted for incorrect answers, and will deal with the subjects studied in the distance learning phase. Each question will have the same value, with the mark obtained being a function of the number of questions answered correctly in relation to the total number of questions asked. It will be necessary to conclude this test, at least, with a minimum of five (5) points.

The final grade of the course will be "PASS", being the grade of the distance learning phase considered only for the access to the phase that will take place at the end of the course, is started later.

During the synchronous phase, the student will have to pass another test on the course content. The questions will be theoretical multiple-choice questions in written format with four possible answers (only one true answer), with no points deducted for incorrect answers. Each question will have the same value, with the mark obtained being a function of the number of questions answered correctly in relation to the total number of questions asked. It will be necessary to conclude this test with at least a minimum of five (5) points. In the event of failing to pass the minimum required, the student will have to take a recovery assessment which, if not passed, will result in the student being dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of public administrations in subgroups A1 or A2 who have responsibilities in the planning, management, administration or maintenance of information and communications technology (ICT) systems, or with their security, may apply for this course.

The following are considered as priorities for selection to the course:

• Be engaged in the planning, management, administration or maintenance of ICT systems, or the security thereof, for a period exceeding two (2) years.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. In the registration process, a username and password are established for connection to the Portal. Before the course is held, students will be provided with the details and instructions for accessing the asynchronous phase by e-mail. The student will have to take into account the following requirements:

• The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.

• The email account must be operational and frequently used.

Subjects - Asynchronous phase

The subjects into which the first phase of the course is divided are listed below, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Digital Principles (Online phase)	- Digital Principles	4,5	4,5	0	Numbers used in Digital Electronics. Binary codes. Basic logic gates: AND, OR, NOT. Circuit Simplification: Diagrams. Basic structures: Flips-Flops. Counters. Shift registers. Types of circuits.
Number Theory (Online phase)	- Number Theory	4,5	4,5	0	Numerical bases. Divisibility. Modular arithmetic. Groups. Rings and Bodies. Rings of polynomials.
Classical Cryptography (Online phase)	- Classical Cryptography	3,5	3,4	0,1	Basic principles of cryptography. Manual encryption procedures. Mechanical cryptographers.

Subjects - Synchronous phase

The subjects into which the second part of the course is divided are listed below, together with their contents and the allocation of teaching hours..

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Theory of cryptography	- Theory of cryptography	5,3	5	0,3	Modern cryptography. Serial encryption. Block cipher. Summary functions. Public key cryptography Cryptography with elliptic curves. digital signature cryptographic protocols Quantum and post-quantum cryptography. Blockchain. Public Key Infrastructure. Side-channel attacks. Cryptographic applications. New lines.
Tempest	- Tempest	0,3	0,3	0	Tempest Phenomenon, Tempest Threat, Countermeasures. Case study.
Crypto Regulations and Security	- Cryptologic Regulations. - Cryptologic Security Policies.	0,2	0,2	0	Use of Certified Encryptors, Employment Procedures, Placement of Security Labels, Key Management, Security Incidents. Secure Verification Codes (CSV) Cryptography for use in the ENS Threats, security measures and action.
Team Evaluation	- FIPS140 assessment. - Common Criteria Evaluation. - LINCE evaluation. - Cryptological evaluation. - TEMPEST evaluation.	0,4	0,4	0	Equipment Security Assessment: FIPS 140-2 Assessment, Common Criteria Assessment, LINCE Assessment, Cryptologic Assessment, Security Assessment, Security Evaluation TEMPEST and zoning.
ICT security and cryptological equipment	- Number teams - ICT security products	0,5	0,4	0,1	National Data, IP and Voice Encryptors. NATO and EU cryptologic equipment. ICT security products CPSTIC
Interconnections	- Interconnection of systems	0,1	0,1	0	Interconnection of systems with different classification.
Miscellaneous Group	- Inauguration and Closing.	0,7	0,5	0,2	Preliminary Examination. Inauguration. Final Examination. Critical Judgement and Closure.

Purpose

The purpose of the “STIC Course - Security in Mobile Communications” is to provide attendees with a detailed and updated vision of the security threats and vulnerabilities that are looming over mobile communications. The course describes in detail the known attacks against the different generations of mobile communications protocols, introducing in each case the basic concepts of architecture and security necessary for the student to fully understand the operation of each attack, with different practical examples and demonstrative videos.

During the course, vulnerabilities associated with the different generations of network and data protocols will be studied: 2G, 3G, 4G and 5G.

Credits / Syllabus Hours

The distribution of the 15 hours of the synchronous phase of the course (1.5 credits) is as follows:

- Theory: 1.3 credits / 13 hours
- Practical: 0.2 credits / 2 hours

Standards and Certificate of Achievement

The training will be carried out in classroom mode, with compulsory attendance at the sessions, or in online mode, in which participants will have to connect to the live broadcast of the classes during the four days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as “COMPETENT”. In the event of not passing the minimum required, the student will be considered as “NOT APT” and will be withdrawn from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

At the end of the course, participants who have successfully completed the course will receive a Certificate as a guarantee of success, of overcoming it.

Addressees

Public employees in subgroups A1, A 2and C1, and the equivalent employment staff, who have responsibilities, at a technical level, in the planning, management, administration or security of information and communications technology systems and who also need to carry out tasks related to mobile communications management environments, information security and security audits for their job, may apply for the course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Mobile Communications Security	- Introduction to mobile communications - 2G communications security - 3G communications security - 4G communications security - 5G communications security	1,4	1,2	0,2	Introduction to mobile communications. Security in 2G communications: Voice and SMS at the radio interface. Voice and SMS in the core network. GPRS/EDGE at the radio interface. GPRS/EDGE in the core network. 3G communications security: Introduction to 3G. Security analysis of the radio interface. Security analysis of the core network. Countermeasures. Security in 4G communications: Introduction to 4G. Implementation of voice calls and SMS. Security concepts. Attacks against 4G. Conclusions. Security in 5G communications: Introduction. Security concepts. Attacks against 5G. Conclusions. Final conclusions.
Miscellaneous Group	- Inauguration and Closing.	0,1	0,1	0	Inauguration. Critical Judgement and Closing.

Purpose

The aim of the **"STIC Advanced Course - Mobile Devices"** is to provide attendees with the necessary knowledge, through a theoretical and practical approach to the most widely implemented platforms (Android and iOS), to understand and analyse the threats existing in mobile devices in order to mitigate them.

At the end of the course, participants will learn about the challenges and opportunities of these platforms, what their weaknesses are and how secure implementations of these devices can be undertaken in their respective organisations through an analysis of both platforms, interaction with applications, the different approaches to their security architecture, the most common threats and an introduction to the forensic analysis of these devices.

Credits / Syllabus Hours

The distribution of the 25 hours of the asynchronous phase of the course (2.5 credits) is as follows:

- Theory: 2.3 credits / 23 hours
- Practical: 0.2 credits / 2 hours

The distribution of the 35 hours of the asynchronous phase of the course (3.5 credits) is as follows:

- Theory: 1.0 credits / 10 hours
- Practical: 2.5 credits / 25 hours

Standards and Certificate of Achievement

As this course is developed in two (2) phases (asynchronous and synchronous), it will be an essential condition to participate in the synchronous phase, to pass the tests corresponding to the exams foreseen during the asynchronous phase in which the knowledge acquired in this phase will be assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the seven (7) days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Public employees of subgroups A1, A2, B and C1, and the equivalent employment staff, who have responsibilities in the planning, management, administration or security of information and communication technology systems and who also need to carry out tasks related to the compliance of their organisation with the National Security Scheme, may apply for the course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems and a working knowledge of network protocols and equipment. It will also be necessary to have advanced knowledge in handling virtualisation environments and average knowledge of Shell Scripting and Java, the following being considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. In the registration process, a username and password are established for connection to the portal. Before the course is held, students will be provided with the details and instructions for accessing the asynchronous phase by e-mail. The student must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Introduction to security on mobile devices (Phase a distance)	- Introduction. Android, iOS and other operating systems. Best practices. Physical access. USB communications. Default configuration. Device encryption.	1,0	0,8	0,2	Introduction to security on mobile devices. Security and physical access. Current communications and threats.
Security on mobile devices (Remote phase)	- Lock screen. Updating of the Operating System and applications. Device encryption. Back-up. Wireless communication capabilities. Mobile applications.	1,5	1,5	0	Recommendations and best practices in the use of mobile devices. Describe best practices. Protection and the safest possible use of mobile devices. Configuration and use of existing protection mechanisms.
Security on mobile devices	- Issues and opportunities. Mobile device platform analysis. Mobile application interaction. Security model and architecture. Analysis of mobile devices. Unlocking, rooting and jailbreaking. Architecture of storage and file system. Reverse engineering obfuscated applications. Analysis of static applications. Analysis of Android applications. Geolocation and spoofing. USB, Bluetooth, WiFi and NFC. Malware attacks and threats. Introduction to the forensic analysis of the mobile device.	3,3	0,8	2,5	Secure deployment of mobile devices. Weaknesses in mobile devices. Exploiting weaknesses. Permission management models in iOS and Android. Code signing weaknesses in Android. Application execution. Latest security improvements in Android and iOS. Android and iOS application interaction. Application protection through permissions and signatures. Security model and architecture. Lab: use of emulators, analysis and interaction with Android Debug Bridge, interaction via Activity Manager. iOS Jailbreak. Unlocked Bootloaders. Android Exploits. Data storage architecture and file system. File system structure Data decoding. Laboratory: Reverse engineering obfuscated applications. Laboratory: Analysis of static applications. Laboratory: Analysis of Android applications. Geolocation and Spoofing. USB, Bluetooth, WiFi and NFC communications. Laboratory: Network manipulation. Laboratory: SSL/TLS attacks. Laboratory: Web attacks. Laboratory: RAT. Malware threats. Introduction to mobile device forensics. Conclusions and references.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC - Wireless Networks Course"** is to provide participants with the knowledge and skills necessary to be able to decide which wireless technologies are most appropriate for each specific organisation, and to implement and make optimal use of each of the capabilities they offer in order to contribute efficiently to the security of the organisation as a whole.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

This course is open to staff with responsibilities at technical level in planning, management, administration or maintenance of information and communications technology systems, or with their security.

Attendees will be expected to have a minimum administrative level knowledge of Linux and Windows systems, as well as basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- Have previously completed the STIC Basic Course - Network Infrastructure developed by the National Cryptologic Centre.
- Activity related to the administration of the network infrastructure associated with Information and Communication Technology (ICT) systems.
- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the CCN.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- WMAN communication. - WLAN communication. - WPAN devices.	2,4	0,9	1,5	Inter-site communication (WMAN). Pre-WIMAX technology. Authentication by means of Digital Certificates. Communications Encryption. Use of VLAN. Intra-site communications (WLAN). Wireless Network for Internal Access. Wireless Network for Roaming Clients. Access Point Distribution. 802.1X protocol. Classical Attacks on Wireless Networks. Mobile Devices Personal Area Network (WPAN). Bluetooth Personal Area Network.
Miscellaneous Group	- Inauguration and Closing.	0,1	0,1	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC - Cybersurveillance Course"** is to provide participants with the necessary knowledge to understand and define information needs at each step of the Open Source Information gathering (OSINT) spectrum, with a particular focus on the OSINT approach as it applies to the development of cyber-surveillance work.

The programme takes the format of a self-contained course with the purpose of providing attendees with a practical overview of OSINT knowledge and procedures for conducting cyber-surveillance work, so that attendees have access to a useful set of minimum techniques and methodologies to start performing specific tasks, a sort of toolbox for OSINT cyber-surveillance.

In this context, the course has been designed to combine methodology with technology within an OSINT research process; to develop the ability to define tactical utilities for shortening search processes, tracking information elements of interest, and monitoring specific digital scenarios; the acquisition of new web habits of advanced use of social media searches; the systematisation of procedures for the analysis and evaluation of digital scenarios and identities based on the information obtained; as well as the practical approach to research and the elaboration of cyber-surveillance reports.

The philosophy of knowledge transfer, in terms of the procedures, techniques and technologies studied, in which

The course is part of Preventive Cybersecurity and Passive Cyber Defence.

Credits / Syllabus Hours

The distribution of the 25 hours of the asynchronous phase of the course (2.5 credits) is as follows:

- Theory: 2.3 credits / 23 hours
- Practical: 0.2 credits / 2 hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 0.7 credits / 7 hours
- Practical: 1.8 credits / 18 hours

Standards and Certificate of Achievement

As this course is developed in two (2) phases (asynchronous and synchronous), it will be an essential condition to participate in the synchronous phase, to pass the tests corresponding to the exams foreseen during the asynchronous phase in which the knowledge acquired in this phase will be assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the five (5) days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Public employees in subgroups A1, A2, B and C1, and the equivalent employment staff, who have responsibilities in the planning, management, administration or security of information and communication technology systems and who also need to carry out cyber-surveillance, investigation and reporting tasks related to the detection of threats in social networks for their job, may apply for the course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Commercial means (COTS) will be used, available to any Internet user, so that communications and activities can go unnoticed within the normal traffic of a user on the Internet, avoiding the signalling of the activity to be carried out.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. In the registration process, a user name and password are established for connection to the Portal. Before the course is held, students will be provided with the details and instructions for accessing the asynchronous phase by e-mail. The student must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Introduction to cyber-surveillance (Distance learning phase))	- Introduction to cyber-surveillance. Open source and social media collection techniques. Management of applications to generate cyber-intelligence.	1,0	0,8	0,2	Introduction to cyber-surveillance. Open source and social media intelligence gathering techniques. Management of applications for open source intelligence generation.
Cyber crisis management (Remote phase)	- Introduction. What is a crisis? Definition and management of cybercrisis. Good practices in cyber crisis management. Case studies.	1,5	1,5	0	Best practices in cybersecurity crisis management. Definition of crisis. Definition of cyber crisis. Cyber crisis management. Best practices in cyber crisis management.
Cybersurveillance	- General concepts and OSINT methodology. Obtaining OSINT. Social Networking. Cybersurveillance. Anonymisation. Associated tools. Preparation of reports.	2,3	0,5	1,8	Introduction. General concepts of the working environment. OSINT methodology. Obtaining OSINT: Searches. Social Networking. Cybersurveillance: Definition and Objectives. Cyberprotection and Anonymisation in cybersurveillance. Social Network Architecture. Social Networking APIs. Google Dorks. Free tools for monitoring and research. Practical approach to content tracing. Practical approach to profiling a digital identity. Identification of Bots in Social Networks. Elaboration of reports from cyber-surveillance. Organisation of a cyber-surveillance unit. Use cases. Digital Observatory.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The aim of the **"Basic ICT Security Audits Course"** is to provide participants with the necessary knowledge and skills to be able to check and audit, with sufficient guarantee, the security aspects of ICT systems in each specific organisation, as well as to verify and correct processes and implementations.

Credits / Syllabus Hours

The distribution of the 20 hours of the asynchronous phase of the course (2 credits) is as follows:

- Theory: 2.0 credits / 20 hours

The distribution of the 50 hours of the synchronous phase of the course (5 credits) is as follows:

- Theory: 2.6 credits / 26 hours
- Practical: 2.4 credits / 24 hours

Standards and Certificate of Achievement

As this course is developed in two (2) phases (asynchronous and synchronous), it will be an essential condition to participate in the synchronous phase, to pass the tests corresponding to the exams foreseen during the asynchronous phase in which the knowledge acquired in this phase will be assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the ten (10) days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2, B or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. In the registration process, a username and password are established for connection to the Portal. Before the course is held, students will be provided with the details and instructions for accessing the asynchronous phase by e-mail. The student must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Course on ENS Audits (Phase asynchronous distance)	- Information Systems Audits. - General concepts of ENS Audit and Certification. - Development and execution of an audit.	2,0	2,0	0	Definition of audit. Audit criteria. Preliminary definitions. Essential principles. Audit programme. Implementation. Definition of objectives, scope and criteria. Results management. Scope. Technical competence. Resources of the Certification Body. Audit time. Audit findings. Remote certification. Services shared. Conformity mark. Certification in exceptional situations. Obligations of the Entities. Provisional approval of conformity. Scope and purpose. Audit team. Planning. Evidence. Development and presentation of the findings. Presentation of the report. Final opinion.
STIC Technical Measures	- ICT Security Audits. Audit Methodology. ENS Inspections. STIC Inspections	4,8	2,4	2,4	Introduction to Audits. CCN-STIC Guide 303. Audit Methodology. Compliance with Organisational aspects. ENS Level Inspection 3. STIC Inspection. Technical Inspection of Black Box Level 5. Technical Inspection of Application Levels 4 and 5. STIC Inspections: Case Studies. Report Models. Executive Report.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Mode: Online tutored

- Asynchronous phase: 20 hours
- Synchronous phase: 50 hours

Purpose

The aim of the **"Advanced ICT Security Audits Course"** is to provide participants with the knowledge and skills necessary to be able to test and inspect with a higher level of specialisation applications and infrastructures where it is necessary to get to know the surface of exposure to vulnerabilities and existing threats by means of White Box and Black Box security tests.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2 or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- To have previously completed the Basic ICT Security Audits Course.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- Pentesting: External Networks and Services - Web Services Audit - Systems Audit	2,3	0.8	1,5	Pentesting. Footprinting techniques. Fingerprinting techniques. Analysis of Vulnerabilities. Attacks against Web Services. Analysis of Servers. System Security Analysis. Attacks on Infrastructures. Exploits. Vulnerability Exploitation with Metasploit Framework.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC Accreditation Course - Operating Systems"** is to provide attendees with the necessary knowledge to be able to check, with sufficient guarantee, the security measures necessary to protect MS Windows and Linux operating systems.

In particular, secure administration and implementation, as well as tools and configurations to reduce the exposure surface of corporate systems, taking as a reference the aspects observed in the various CCN-STIC guides associated with the aforementioned operating systems.

As this is an accreditation course, the regulations contained in the CCN-STIC series will be used as a frame of reference implementing the security settings defined in the aforementioned guides.

Credits / Syllabus Hours

The distribution of the 25 hours of the asynchronous phase of the course (2.5 credits) is as follows:

- Theory: 2.3 credits / 23 hours
- Practical: 0.2 credits / 2 hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

As this course is developed in two (2) phases (asynchronous and synchronous), it will be an essential condition to participate in the synchronous phase, to pass the tests corresponding to the exams scheduled during the asynchronous phase in which the knowledge acquired in this phase will be assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the five (5) days of the course. During the sessions, a series of practical exercises will be carried out to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Public employees of subgroups A1, A2, B and C1, and the equivalent employment staff, who have responsibilities in the planning, management, administration or security of information and communication technology systems and who also need to carry out tasks related to the compliance of their organisation with the National Security Scheme, may apply for the course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- Activity related to the administration of Information and Communication Technology (ICT) systems under Windows and Linux environments.
- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Access to the course (on-line phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. The student must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Introduction to Systems Accreditation (Distance Learning Phase)	- Introduction to system accreditation. Continuous improvement approach. Accompaniment, support and maintenance of accreditation.	1,0	0,8	0,2	Introduction to system accreditation. Continuous improvement approach (short, medium and long term objectives). Analysis of latest related abstracts. Adaptation to the sensitive information handling ecosystem. The continuous security model, as opposed to more rigid traditional evaluation mechanisms, Risks to be assessed so that sensitive information is stored in Cloud services. The figure of the accompanying companies.
STIC Basic Course Security in Windows Environments	- Operating systems. Administration and security. Active Directory and policies.	1,5	1,5	0	Introduction to the management of the Windows Server O.S. and Windows clients. Basic administration. Local system security. Active Directory. Group policies. Associated CCN-STIC guides.
STIC accreditation course - Operating Systems	- Windows Systems Security Administration. Active Directory security and group policies. Linux Systems Security Administration. Additional Security Measures. Associated CCN-STIC Guides.	2,3	0,5	1,8	Security Administration in Windows Systems: Security risks in roles and characteristics of Windows Server 2016. Assigning permissions to resources. User account control (UAC) and elevation of privileges. Network security (protocols, types, advanced security of Windows Defender). Policies local security. Security based on Active Directory domain services and group policies: Logical structure and implementation of Active Directory. Domain Controllers. Active Directory administration. System management using GPOs. Computer and user policies: security policy management. Security filtering and WMI. Security filtering and WMI. CCN-STIC guides associated with Windows systems. Structure and elements. Security administration on Linux systems: File system and partitions. Shell and GNU commands. Startup, services and Kernel. Secure installation and configuration of services and software components. User and group administration. System logging. Secure management with SSH and web console. Additional security measures: Network connections and firewall restrictions. Control of system services and running processes. File and file system management and protection. Shell scripting. Security and system access management (SELinux). CCN-STIC guides associated with Linux systems. Structure and elements.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC Course - Network Infrastructure Security"** is to provide participants with the necessary knowledge about the main threats that affect the infrastructures and equipment that support communications networks, as well as to know and apply the appropriate measures to guarantee their security. In particular, the aim is to:

- Review basic concepts of local area networks and IP networks, as well as router and switch configuration.
- To understand the main threats affecting the security of routers and switches and, by extension, the networks and services based on them.
- Know and apply basic measures and good configuration practices to mitigate threats, both in access to equipment management and in the data and control plane.
- To know the techniques for secure access to the remote management of equipment by means of virtual private networks.
- Knowing and applying security tools for scanning networks and systems, as well as performing security audits.

Credits / Syllabus Hours

The distribution of the 15 hours of the asynchronous phase of the course (1.5 credits) is as follows:

- Theory: 1.5 credits / 15 hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

As this course is held in two phases (asynchronous and synchronous), in order to participate in the synchronous phase, it is essential to pass the tests corresponding to the exams scheduled during the asynchronous phase, in which the knowledge acquired in this phase is assessed.

The synchronous phase will be carried out in online mode, so participants will have to connect to the live broadcast of the classes during the five (5) days of the course. During the sessions, a series of laboratory practices will be carried out on the contents taught, which will make it possible to assess whether they have obtained adequate knowledge to pass the course and be considered as "COMPETENT". If the student does not pass the minimum required, he/she will be considered "NOT APT" and will be withdrawn from the course.

The final grade of the course will be "PASS", being the grade of the asynchronous phase considered only for the access to the synchronous phase, which starts later.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Public employees in subgroups A1, A2, B and C1, and the equivalent employment staff, who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with the security of the same, may apply for the course.

Participants will be expected to have a minimum knowledge of operating systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- Activity related to the administration of the network infrastructure associated with Information and Communication Technology (ICT) systems.
- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Course access (Asynchronous phase)

In order to participate in the asynchronous phase, the student must be a registered user of the ANGELES portal (https://angeles-privado.ccn-cert.cni.es/), where the e-learning platform is located. The student must take into account the following requirements:

- The e-mail account used for communication between the tutor and the students can be a personal or work one, but it must match the one indicated in the online application.
- The email account must be operational and frequently used.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures (Distance Learning Phase)	- STIC Network Infrastructure Security Course	1,5	1,5	0	Computer networks. Internet. Applications. Transport protocols. IP networks. Addresses and prefixes. Routers. Forwarding of datagrams. IP and ICMP protocol. NAT. Routing in IP networks Static routing Dynamic routing protocols. OSPF. BGP. Local Area Networks (LAN). Switches/Ethernet switches. Learning algorithm. VLAN. Routing in LAN networks: STP. Basic notions of network equipment configuration.
STIC Technical Measures	- Introduction to network infrastructure security. - Security in local area networks. - Identification, authentication and access control. Virtual private networks. - Security in IP networks. - Equipment security audits.	2,3	0,8	1,5	Basic security concepts. Types of threats. Security policies. Anatomy of an attack. Security in the configuration and management of network equipment. Concept of «hardening». Secure access to management. Basic recommendations: management of configurations, software updates, aggregation logs, etc. Monitoring. Description of the practice scenario. Secure configuration of network equipment and use of security tools (practical). Threats and attacks on switches. Saturation of CAM tables. MAC address spoofing. ARP spoofing. DHCP starvation/spoofing. VLAN hopping techniques: switch spoofing and double tagging. LAN routing: Spanning Tree Protocol attacks. Security measures to mitigate attacks. Security in local area networks (practical). Basic identification and authentication mechanisms. Access control. Authentication protocols. 802.1x. Centralised user authentication. RADIUS. Network access control systems: Network Access Control (NAC). Single Sign On (SSO) solutions. Virtual Private Networks (VPN). Secure configuration of remote access with VPN and RADIUS as authentication server (practical). Threats and attacks on routers. IP spoofing (IP spoofing). Denial of service (DoS) attacks. Security in routing protocols: authentication. Countermeasures: Unicast Reverse Path Forwarding (URPF), access lists (ACL), flow monitoring: NetFlow/sflow. Routing techniques to mitigate DoS attacks. Configuring security measures in IP networks (practical) Tools for conducting equipment safety audits. ROCIO tool. Conducting audits with ROCIO and other tools (practical).
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Mode: Online tutored

- Asynchronous phase: 15 hours
- Synchronous phase: 25 hours

Purpose

The aim of the **"STIC Course - Web Application Security"** is to provide participants with a detailed, up-to-date and practical overview of the security threats and vulnerabilities affecting Web infrastructures, environments and applications. The different modules include a detailed description of the vulnerabilities studied, attack techniques, defence mechanisms and security recommendations, including numerous demonstrations and practical exercises.

The reference framework will be the CCN-STIC series regulations, implementing the security configurations defined in the CCN-STIC-412 guide, security requirements for Web environments and applications.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will not be able to take part in the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of public administrations in groups A1, A2 or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of systems and networks, web environments and web application developers may apply for this course.

Participants will be expected to have a minimum administrative knowledge of Windows and Linux systems, as well as a basic knowledge of network protocols, with the following being considered as priorities for selection to the course:

- Have previously completed the Basic Course on ICT Security Audits developed by the National Cryptologic Centre (CCN).
- Have previously completed the STIC - Firewall course developed by the National Cryptologic Centre (CCN).
- Have previously completed the STIC - Intrusion Detection Course developed by the National Cryptologic Centre (CCN).
- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the CCN.

- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- Introduction to threats in web applications. - Web Protocols. - Web analysis and manipulation tools. - Attacks on web environments. - Web Authentication and Authorisation Mechanisms. - Session Management. - SQL Injection. - Cross-Site Scripting (XSS) - Cross-Site Request Forgery (CSRF).	2,4	0,9	1,5	Web application architectures. Web Application Security Analysis Methodology. Web Application Firewalls. HTTP/ HTML7SSL/TLS protocols. Recognition of the Web environment. Web platform vulnerabilities. Web attack tools. Web manipulation proxies. Directory traversal. Code and content injection. Web Authentication (basic, certificates) and Web Authorisation. ID and token management for session. Cookies. Types of injection (SQL, LDAP). Types of XSS. Evasion of XSS detection. CSRF attack. Security Recommendations
Miscellaneous Group	- Inauguration and Closing.	0,1	0,1	0	Inauguration. Critical Judgement and Closing.

Purpose

The aim of the **"STIC - Early Detection Course"** is to provide attendees with the necessary knowledge to adequately manage ICT security incidents faced by an organisation through the use of Early Warning Systems and other solutions that the CCN-CERT makes available to Public Administrations.

Credits / Syllabus Hours

The distribution of the 20 hours of the synchronous phase of the course (2.0 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1 credit / 10 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

At the end of the course, attendees who have successfully completed the course will obtain an annotation of the course on their personal file as a guarantee of success.

Addressees

Staff in the service of Public Administrations in groups A1, A2 or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- Introduction to Incident Management - Detection - Use cases in early incident detection - Early Warning Systems - GLORIA Tool - Case studies	1,9	0,9	1,0	Introduction to incident management: CCN-CERT tools. Incident management phases. Detection: Types of environments. Types of detection. Pyramid of Pain. Risks. Use cases: Definition of scenarios. Development. Validation and deployment. Early Warning Systems. GLORIA Tool: Procurement - Argos. Correlation - Triton. Event Console - EMAS. Statistics - Hera. Asset map (ICS). Automation. Full case study.
Miscellaneous Group	- Inauguration and Closing.	0,1	0,1	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC Course - Cybersecurity Incident Management"** is to provide attendees with the necessary knowledge to properly manage ICT security incidents faced by an organisation by using the CCN-CERT tools.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2 or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have previously completed the Basic Course on ICT Security Audits developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- Early Warning System - LUCIA Tool - REYES Tool - CARMEN Tool - Case Studies	2,3	0,8	1,5	Introduction to incident management. LUCIA Tool: Introduction to the tool, RTIR concepts, workflows, instance synchronization. REYES tool: Indicators of compromise, export of SNORT, YARA or IOCs rules, introduction of malware samples, automation of tasks and processes using the REST API. CARMEN Tool: Users and roles, basic filters, use of lists, compromise indicators, external movement analysis (HTTP, DNS, SMTP), lateral movement analysis (NetBIOS), analyzers and indicators, plugin creation. Case Studies: Threat Identification and Detection
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC - Advanced Cybersecurity Incident Management Course"** is to provide attendees with the necessary knowledge to enable the performance of a team of security analysts in the process of investigating complex incidents through the use of the CCN-CERT's own solutions for the acquisition, processing and analysis of network traffic.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of public administrations in groups A1, A2 or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- Have previously completed the course (STIC) - Cybersecurity Incident Management developed by the National Cryptologic Centre.
- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have previously completed the Basic Course on ICT Security Audits developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- REYES Tool - CLAUDIA Tool - CARMEN Tool - Case Studies	2,3	0,8	1,5	REYES tool: introduction and concepts. Integration with other CCN-CERT solutions and its possibilities. CLAUDIA tool: introduction and concepts. Integration with the CARMEN tool. CARMEN tool: users and roles, basic filters, use of lists, indicators of compromise, external movement analysis (HTTP, DNS, SMTP), lateral movement analysis (NetBIOS), analyzers and indicators, creation of plugins. Case Studies: Identification and detection of threats, use of support tools, detection of anomalies for the creation of IOCs, search for APTs, analysis of memory dumps.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC - Memory Analysis Course"** is to provide participants with the knowledge and skills necessary to carry out, with sufficient guarantee, the investigation of security incidents using forensic memory analysis techniques.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credit / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

The course will be carried out synchronously, which means that participants will have to do a series of practical exercises to assess whether they have obtained the appropriate knowledge to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be dropped from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2 or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Participants will be expected to have a minimum administrative knowledge of Linux and Windows systems, as well as basic knowledge of network protocols and equipment, with the following priorities being considered for selection to the course:

- Have previously completed the STIC Course on Cybersecurity Incident Management (CCN-CERT Tools).
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
STIC Technical Measures	- Forensic Analysis on Windows Systems - Introduction to Windows Internals - Forensics on Windows Systems - Ring 3 - Forensics on Windows Systems - Ring 0 - Forensics in other sources and final challenge	2,3	0,8	1,5	Introduction to Memory Forensics. Windows architectures. Volatility. RAM Acquisition. Analysis methodologies. Unstructured Memory Analysis. Process Internals. Volatility listing modules. Pool memory. Network connections. Code injection. User Artifacts in memory. Kernel Objects Other memory blocks in Windows. Athena CTF Challenge.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

Purpose

The purpose of the **"STIC - Cyber Intelligence Course"** is to provide attendees with the necessary knowledge, through a theoretical-practical approach, about the concepts related to cyber intelligence, what is the role of an intelligence analyst and what activities should be developed when identifying and analysing the intelligence associated with threats through the study of the diamond model and to be able to carry out investigations through OSINT techniques.

Upon completion of the course, participants should be familiar with the basic concepts related to cyberintelligence, the different typologies of existing intelligence sources, identify techniques and tactics associated with groups of attackers, the collection of indicators of compromise and their value, and be able to conduct basic investigations.

Credits / Syllabus Hours

The distribution of the 25 hours of the synchronous phase of the course (2.5 credits) is as follows:

- Theory: 1 credits / 10 hours
- Practical: 1.5 credits / 15 hours

Standards and Certificate of Achievement

As this course is carried out in synchronous mode, attendance or connection to all the scheduled sessions will be compulsory, as well as a series of practical exercises that will make it possible to assess whether the appropriate knowledge has been obtained in order to pass the course and be considered as "COMPETENT". In the event of not passing the minimum required, the student will be considered "NOT APT" and will be withdrawn from the course.

Any modification of the above, due to circumstances that so require, shall be reflected in the Act of Completion of the course.

Addressees

Staff in the service of Public Administrations in groups A1, A2, B or C1 who have responsibilities, at a technical level, in the planning, management, administration or maintenance of information and communications technology systems, or with their security, may apply for this course.

Attendees will be expected to have a minimum knowledge of Linux and Windows systems, as well as a basic knowledge of network protocols and equipment, with the following being considered as priorities for selection to the course:

- To have previously completed the Information and Communications Technology Security Course (STIC) developed by the National Cryptologic Centre.
- Have completed courses related to IT or IT security.
- Have responsibilities, at a technical level, in the implementation or operation of ICT systems or in the management of the security of such systems for a period of more than one (1) year.

Subjects

The following are the subjects into which the course is divided, with an expression of the contents and allocation of teaching hours.

Subject designation	Subjects that make up the subject	CREDITS			Brief Description of Content
		TOT	TEO	PRA	
Cyberintelligence	- Introduction to cyber-intelligence. - Intelligence life cycle. - Concepts: information, data and intelligence. - Intelligence sources. - Collection and sorting information. - Indicators of Commitment. - Diamond Model and classification of actors. - OSINT research techniques.	2,3	0,8	1,5	Concepts of cyber-intelligence OSINT, IMINT, SOCMINT, HUMINT, GEOMINT, MASINT, MASINT Bigdata associated with intelligence gathering. Information classification and intelligence generation. Engagement indicators, typology, how to generate them and where to apply them. Diamond model associated with the intelligence for the identification of different actors. Research using OSINT techniques. OSINT in search engines. Image analysis. Searches in RRSS.
Miscellaneous Group	- Inauguration and Closing.	0,2	0,2	0	Inauguration. Critical Judgement and Closing.

3. *Online* training

The Ángeles platform of the National Cryptologic Centre (www.ccn.cni.es) offers several types of online courses depending on the user's profile. It is possible to register through the Cl@ve system (with DNI/e, electronic certificate, or Cl@ve PIN) and allows the export of the student's online training file, which specifies the hours of training received, as well as the courses and awareness-raising sessions carried out on the platform.

- Cybersecurity basics
- Linux basics
- INES (National Report on the State of Security)
- STIC Basics - Security in Windows environments
- Risk Analysis and Risk Management of the Information Systems
- National Security Scheme
- Information and Communications Technology Security (ICTS)

ángeles
Formación, capacitación y talento en ciberseguridad

4. Learning via *streaming*

The CCN-CERT's VANESA solution is a **platform for broadcasting live training sessions,** which allows hundreds of people to attend from anywhere in the world.

Furthermore, as an added value and in order to achieve a wide dissemination of the broadcasted content, Vanesa keeps the recordings and the material used, thus allowing its subsequent viewing.

</vanesa>

- CCN-CERT Solutions
- Malicious Code
- Mobile communications
- E-mail address
- Firewall
- Mobile devices
- ENS
- ENS Meetings
- Forensic
- STIC Products
- Third-party solutions
- Web
- Windows

5. ATENEA School

Atenea School is a platform of computer security challenges, composed of different guided challenges and supporting training material, which aims to encourage the learning of less knowledgeable or non-expert users in the field.

It has been developed by the CCN-CERT, as part of the Atenea platform, with the The conviction that learning can be stimulated through challenges.

6. ELENA. Surveillance Techniques Simulator

This is the CCN-CERT platform for practising techniques, tactics and procedures in cyber-investigation work. It allows users to take on the role of an analyst in a simulated investigation environment based on real situations, which makes it possible to develop and put into practice the techniques, tactics and procedures necessary to carry out cyber-investigation work.

System

- **Simulated real-life**
- **With a variety of scenarios**
- **Intuitive and robust**
- **Tested by experts**

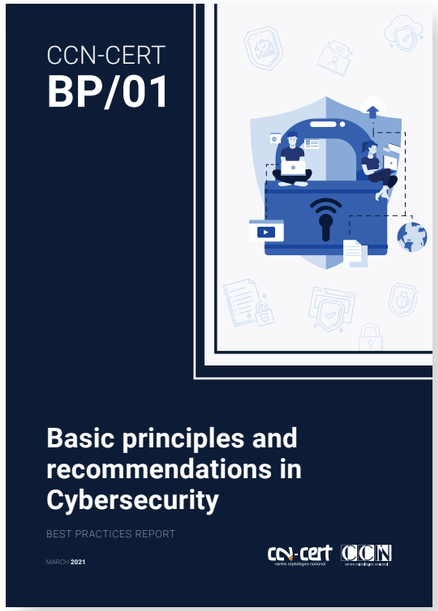
Includes

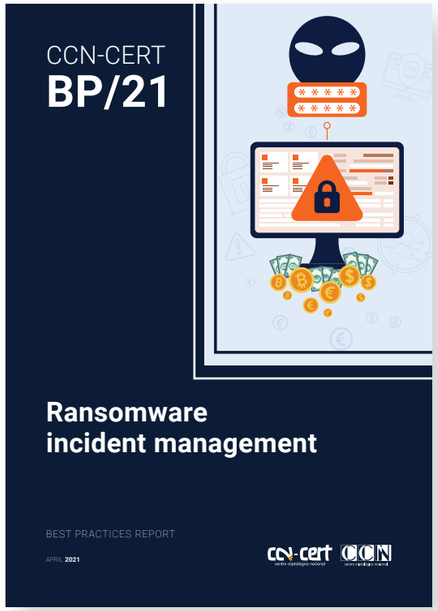
- **All necessary resources from the outset**
- **Detailed Statistics**
- **Ranking of best participants**

7. Publications

Aware of the possible risks that may affect the security of Information and Communication Technologies, the National Cryptologic Centre periodically prepares **Best Practice reports** with the aim of guiding users in the secure use of new technologies.

These reports, accessible from Angeles, analyse the existing vulnerabilities or threats, offer guidelines to mitigate or prevent the incident from affecting those who use the technologies covered by the report and, finally, it includes a decalogue of security recommendations to be implemented in order to avoid the consequences derived from these threats or vulnerabilities.





1 **BP/1** – Cybersecurity Principles

2 **BP/2** – Electronic mail

3 **BP/3** – Mobile devices

4 **BP/4** – Ransomware

5 **BP/5** – Internet of Things (IoT)

6 **BP/6** – Web browsers

7 **BP/7** – HTTPS implementation

8 **BP/8** – Social Networking

9 **BP/9** – Firewall DoS Protection

10 **BP/10** – CDN Recommendations

11 **BP/11** – Recommendations for corporate WIFI networks

12 **BP/12** – Cryptojacking

14 **BP/14** – Statement of Applicability ENS

15 **BP/15** – Best Practices in Virtualisation

16 **BP/16** – Adobe Acrobat Reader DC Security Recommendations

17 **BP/17** – Mozilla Firefox Security Recommendations

18 **BP/18** – Security recommendations for teleworking situations and reinforcement in surveillance

19 **BP/19** – Google Chrome Security Recommedations

20 **BP/20** – Best Practices in the Management of Cyber crisis

21 **BP/21** – Ransomware Incident Management

22 **BP/22** – Security recommendations for Oracle Database 19C

23 **BP/23** – Security recommendations for DB2 databases

24 **BP/24** – Security recommendations for databases

25 **BP/25** – Security recommendations for DB2 on zOS databases

26 **BP/26** – Microsoft Edge security recommendations

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es