5G TACTIC

5G Trusted And seCure neTwork servICes

Summer School on 5G Network Security

Programme and Travelling Information

Grant Agreement no. 101127973

Digital Europe Programme

Table of Contents

1.1. Course Overview

The EU has identified digital technologies as one of the key elements to address fundamental challenges associated with social and economic goals, such as improving quality of life, sustainable development, and economic growth. In this context, the deployment of 5G technologies, in both public and private environments, creates new opportunities for governments, businesses, and individuals, thanks to its capacity for connectivity, process automation, and the optimization of energy and resource efficiency. To accelerate the penetration of 5G networks in society, the EU has prioritized the deployment of secure 5G networks.

In this context, this course aims to provide training for relevant stakeholders in the deployment and management of 5G systems. The course content covers both technical training in cybersecurity applied to 5G systems, as well as training from a legal perspective within the European cybersecurity framework.

The first block of the course will present the most relevant technical concepts of 5G networks from a cybersecurity perspective, as well as the underlying infrastructure that enables their deployment. Once the technical environment has been introduced, the regulatory framework and the initiatives followed within the EU will be described. A third block will focus on the use of Artificial Intelligence (AI) solutions to ensure the secure operation of these systems. The course will conclude by providing a comprehensive overview of a secure 5G system, building upon the elements previously presented. A significant part of the course will be dedicated to practical activities, particularly during the technical sessions.

The course is aimed at both students of technical disciplines and professionals involved in cybersecurity, network management, and communication systems operation.

1.2. Duration, dates and Venue

- 15 hours
- 22/06/2026 – 24/06/2026
- Universidad de Cantabria, Santander (Spain)

1.3. Instructional and Material Requirements

The course will include both theoretical/descriptive and practical sessions. Generally, the organization will provide all necessary materials for the practical sessions (e.g., software, connectivity, demos). Additionally, students are encouraged to bring their own laptops for the practical activities.

1.4. Registration

To register for the course, follow these guidelines:

1) If you are not member of Universidad de Cantabria, first register as external user here.

2) Complete your registration through the following link.

3) Send the following documents to cv.ceu@unican.es in the next 3 days after your registration:

- Photocopy of a valid ID or passport.
- Bank receipt (if paid in cash at the bank). Please keep the original copy.
- Payment confirmation for transactions made via credit or debit card.
- Supporting documentation for those applying for reduced or ultra-reduced fees

Registrations completed and paid before June 10th have an early bird fee of 50 €. After this deadline, the standard fee of 100 € will apply.

At the end of the course, students who participate in at least 80% of the teaching hours will receive a certificate of attendance issued by the University of Cantabria. Generally, Summer Courses organized by the University of Cantabria are eligible for ECTS credit recognition.

1.5. Programme

Monday

10:00-12:00 **Title:** 5G core network Design

Lecturer: Luis Diez

Summary: This session will comprise both theoretical introduction (1h) and hands on experience (1h).

This session tackles the deployment and configuration of the 5G core network (CN). To that end, first the main elements of the CN will be presented, describing their functionalities. Then, during the activity communication solutions adopted in the 5G CN will be described. It will include the description of the different protocol stacks, as well as the main procedures that take place during registration and communication. In this sense, special attention will be paid to the procedures of the Radio Access Network (RAN) with the corresponding CN entities (i.e. AMF and UPF). Besides, interaction between the UPF and SMF will be also analyzed, taking into consideration the potential isolated deployment of the UPF. The description of the CN entities and procedures will be complemented with hands-on experience where the actual deployment of 5G CN will be conducted. To that end, open source 5G CN implementations (e.g. Open5Gs, Free5GCore, IAO-CN) will be used to analyze both the behavior of different configuration options, the communication traffic, as well as the potential interoperability between entities belonging to different solution.

12:00-12:30 **Break**

12:30-14:30 **Title:** Security enforcement of 5G Core Network

Lecturer: Alberto García

Summary: This session will comprise both theoretical introduction (1h) and hands on experience (1h).

This activity aims to train on how to secure communication in the 5G CN. It will assume knowledge about the 5G CN functionalities and communication solutions and will elaborate on the potential security risks that may appear on the communication between entities, and the consequences over the overall 5G system. Then, the activity will describe attacks over those interfaces that are more likely to be exposed and present the securitization options following the best practices indicated by standardization bodies.

Tuesday

09:30-13:00 **Title:** Security validation of cloud-native MANO

Lecturer: Maksymilian Furmann

Summary: This session will comprise both theoretical introduction (1h) and hands on experience (2h).

This activity focuses on the security validation of an ETSI-compliant MANO platform based on Open Source MANO (OSM) deployed in the PSNC testbed on top of a cloud-native Kubernetes infrastructure. The session introduces the architecture testbed, mapping OSM components to ETSI NFV-MANO functions and explaining their interactions with the underlying VIM and 5G core network functions. Building on this, the activity presents how ETSI NFV Security Assurance Specifications (SCAS) are instantiated for MANO, and how Security Compliance Testing (SCT) and Basic Vulnerability Testing (BVT) are adapted to an open-source, containerised environment. Selected test cases will be analysed and executed, covering account and role management, transport-layer protection, protection of data in transit, unique VNF instance identifiers, as well as automated vulnerability and port scanning of exposed MANO services.

13:00- 14:30 **Lunch break**

14:30-16:00 **Title:** NIS2 Implementation for 5G Infrastructure: Compliance and Security Measures

Lecturer: Cristian Nistor/Valentin Constantinescu

Summary: This session comprises theory (45') and computer practice (45')

This training activity focuses on understanding and implementing NIS2 Directive requirements for 5G infrastructure operators, with specific emphasis on Romanian legislative framework (OUG 155/2024 and Law 124/2025). The session begins with an overview of NIS2 applicability to the 5G sector, mapping directive requirements to network components (Core Network, RAN, Transport, MANO) and identifying essential/important entities under Romanian law. Participants will learn incident reporting obligations, timelines, and procedures for coordinating with national CSIRTs. Building on this foundation, the activity presents practical implementation of Article 21 (NIS2) cybersecurity measures, including risk assessment methodologies, incident handling workflows, supply chain security evaluation, and business continuity planning for 5G network environments. Selected scenarios will be analyzed covering vulnerability disclosure, vendor risk assessment, security policy development, and compliance documentation requirements, providing participants with actionable frameworks for achieving and maintaining NIS2 compliance in their organizations

16:00- 16:30 **Break**

16:30-18:00 **Title:** Standardization and Certification for 5G OPEN RAN systems

Lecturer: Cristian Nistor/Valentin Constantinescu

Summary: This session comprises theory (45') and computer practice (45')

Training about standardization and certification activities going through several important areas like standardization bodies and their role, Open RAN standardization entities, available security standards, available security certification and security assurance methodologies, future of certification, implementation on 5G TACTIC project.

Wednesday

09:30-11:00 **Title:** Machine learning for threat detection in 5G networks

Lecturer: Marija Furdek /Fehmida Usmani

Summary: This session comprises theory (1h) and computer practice (30')

This activity introduces machine learning (ML) methodologies applied to threat detection in modern 5G networks. It focuses on how ML can be leveraged to identify anomalous behaviors, detect attacks targeting the control and management planes, and strengthen the security posture of virtualized and cloud-native 5G systems. Participants will learn about the threat landscape in 5G, including signaling attacks, data-plane anomalies, API exploitation, and poisoning of monitoring streams and how ML models can be trained to detect these threats in real time.

The activity covers supervised and unsupervised ML approaches, and emerging methods such as graph-based learning and federated learning. To complement the theoretical material, the activity incorporates a guided Jupyter notebook exercise where participants will work with simplified monitoring data, train baseline ML classifiers and anomaly detection models, and visualize detection outcomes. This hands-on practice provides an end-to-end view of how ML techniques are applied in operational 5G-threat-detection pipelines. The training concludes with best practices for robust, explainable, and adversarially resilient ML models in 5G cybersecurity.

11:00-11:30 **Break**

11:30-13:00 **Title:** Attack mitigation in 5G Lifecycle Management

Lecturer: Fehmida Usmani/ Marija Furdek

Summary: We discuss the prerequisites and techniques for intelligent network lifecycle management. This activity introduces security threats and mitigating techniques associated with the full lifecycle management (LCM) of 5G services. It focuses on the MANO and service-orchestration layers, which are responsible for instantiating, scaling, migrating, and retiring virtual network functions (VNFs). The training first presents the main vulnerabilities emerging from management interfaces/APIs, VNF placement logic, and AI/ML-assisted monitoring pipelines. Participants will learn how these vulnerabilities can compromise the reliability, integrity, and availability of the 5G platform.

The activity then introduces mitigating measures, including:

- AI/ML-based attack detection applied to NFV-MANO interfaces,

- Secure and geo-aware VNF placement/migration policies,

- Robustification of AI/ML models used in LCM (e.g., anomaly detection, resource prediction).

A short hands-on demonstration using synthetic telemetry in a Jupyter notebook may also be included, showing how manipulated or poisoned monitoring data can impact LCM decisions and how ML-based anomaly detection can be used to protect orchestration workflows.

13:00-14:30 **Lunch break**

14:30-16:30 **Title:** 5G Security Architecture

Lecturer: Anna Tzanakaki

Summary: This activity will provide an introduction to the overall 5G system architecture, with a particular emphasis on the principles, interfaces, and deployment models of Open RAN (O-RAN). Participants will gain a foundational understanding of how open, disaggregated, and interoperable architectures reshape mobile networks and the associated security considerations.

The second part of the training will focus on security consideration in 5G systems and their architectural implications. Modern 5G deployments face a wide spectrum of security risks that are expected to intensify considerably with the advent of 6G. As the industry moves towards open solutions such as O-RAN, there is an increasing need to enhance equipment interoperability and strengthen standardisation efforts, particularly with respect to security objectives. At the same time, emerging 6G technology features introduce additional and more complex security challenges.

Other aspects that will be addressed in this activity will address the fact that 5G and future 6G infrastructures will become significantly more intricate, operating with vast volumes of operational parameters. To manage this complexity, networks will rely heavily on AI-enabled automation to optimise performance and maintain reliable operation. Achieving this vision requires platforms capable of collecting and processing large amounts of data while ensuring strict data privacy, security, and trust guarantees. AI/ML techniques will play a central role not only in network optimisation but also in enhancing the security posture of the entire system.

Finally, a discussion on advanced monitoring capabilities, continuous security assurance mechanisms, and robust processes for cybersecurity threat intelligence sharing—particularly important in multi-vendor and multi-operator environments enabled by O-RAN will be provided. The tutorial will explore these challenges and introduce participants to the emerging security frameworks, tools, and best practices shaping next-generation open mobile networks.

1.6. Lecturers

LUIS FRANCISCO DIEZ FERNÁNDEZ

Position: Assistant Professor (PPL). **Affiliation:** Universidad de Cantabria, Santander (Spain)

Short CV: Luis Diez is an Associate Professor at the University of Cantabria, Spain, where he is with the Communications Engineering Department. He has been involved in international belonging to the frameworks FP7, H2020, Horizon Europe and ECCC. As for teaching, he has supervised 50 B.Sc. and M.Sc. thesis, and he teaches in courses related to cellular networks, network dimensioning, and service management. His research focuses on future network architectures, resource management in wireless heterogeneous networks, and IoT solutions and services. He has published above 85 scientific and technical papers in those areas. He has served as TPC member and reviewer in a number of international conferences and journals.

ALBERTO ELOY GARCÍA GUTIÉRREZ

Position: Assistant Pofessor (PCD) **Affiliation:** Universidad de Cantabria, Santander (Spain)

Short CV: Alberto Eloy García Gutiérrez is a professor and researcher in Telematics Engineering, specialized in next-generation networks, IP/mobile network planning, and traffic and cost models for multimedia services. His work covers NGN/NGI, VoIP and convergent multiservice networks, providing a strong technical basis to address 5G cybersecurity challenges. He has participated in multiple European projects (Euro-NGI, Euro-FGI) and collaborations with operators and vendors focused on design, dimensioning and regulation of advanced infrastructures. He is co-author of works on security protocols in distributed services and of an Internet of Things journal article on using blockchain to enable a highly scalable IoT data marketplace, aligned with integrity, traceability and data protection in large-scale 5G/IoT ecosystems. He also has extensive experience as a lecturer and trainer on advanced networks, QoS and virtualized environments, which is key to discussing 5G cybersecurity from an integrated network-service perspective.

MAKSYMILIAN FURMANN

Position: Telecommunications Specialist **Affiliation:** Poznan Supercomputing and Networking Center (PSNC), Poznan (Polonia)

Short CV: IT specialist at the Poznan Supercomputing and Networking Center (PSNC), holding an M.Sc. degree in Computer Science and Telecommunications from Poznan University of Technology. He is the coordinator of 5G technologies at PSNC and is currently involved in the national PL-5G Laboratory, the Polish 5G Research Infrastructure, which provides an advanced environment for experimentation, validation, and development of 5G solutions.

CRISTIAN NISTOR

Position: Open Source Analysis Expert for Cybersecurity Risks and Threats **Affiliation:** The Romanian National Cyber Security Directorate (DNSC), Bucharest (Romania)

Short CV: Cristian Nistor is an Open Source Analysis Expert at Romania's National Directorate for Cybersecurity (DNSC) with over 24 years of IT experience. He holds Microsoft certifications (Azure Administrator, DevOps Expert) and IRCA ISO/IEC 27001:2022 Lead Auditor certification. He contributes to EU cybersecurity projects including ENDURANCE (critical infrastructure protection), 5G-TACTIC (telecommunications security), aSIEMmetry, and INTERSOC (interconnected SOCs). His work focuses on cybersecurity risk assessment, threat intelligence analysis, vulnerability management, and compliance with Romanian cybersecurity legislation, particularly OUG 155/2024 (NIS2 implementation). Cristian has experience in OSINT analysis and coordinated inauthentic behavior detection, having analyzed bot networks in social media contexts. His role combines practical threat analysis with understanding regulatory frameworks applicable to critical infrastructure operators.

VALENTIN CONSTANTINESCU

Position: Advisor to the Director of The Romanian National Cyber Security Directorate **Affiliation:**The Romanian National Cyber Security Directorate (DNSC), Bucharest (Romania)

Short CV: With more than 15 years of experience in Telecom domain most of them in leading or project management position I have managed to gain a multi domain expertise that allows me to have an end to end view about this industry and to find all the time the best business solutions for assuring customer needs. Adding almost 5 years of security expertise completes the picture of nowadays needs in a digital services domain assuring the knowledge to identify not only the right solutions for assuring quality of the provided services but also the right level of security for them.

FEHMIDA USMANI

Position: Postdoc Researcher **Affiliation:** Chalmers University of Technology, Gothenburg (Sweden)

Short CV: Fehmida Usmani received the Ph.D. degree in Information Technology from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, in 2024. She is a Postdoctoral Researcher at Chalmers University of Technology, Gothenburg, Sweden, where she works on machine-learning-driven solutions for next-generation optical networks and fiber-optic sensing. Previously, she held research positions at Politecnico di Torino, Italy, both as a Visiting Researcher (2022–2023) and a remote Researcher (2023–2025), and served as an Assistant Professor at the National University of Computer and Emerging Sciences, Pakistan. Her research interests include machine learning for optical network monitoring, quality-of-transmission prediction, anomaly and fault detection, and event sensing using optical network measurements. She has authored over 30 peer-reviewed publications in leading journals and conferences, including Journal of Lightwave Technology, IEEE Access, OFC, ONDM, and ICTON. Dr. Usmani is a member of IEEE, Optica, and SPIE, and is the recipient of the Corning Women in Optical Communications Scholarship from Optica.

MARIJA FURDEK

Position: Associate Professor **Affiliation:** Chalmers University of Technology, Gothenburg (Sweden)

Short CV: Marija Furdek received the Ph.D. degree in telecommunications from the University of Zagreb, Croatia, 2012. She is an Associate Professor at Chalmers University of Technology, where she joined in 2019 as an Assistant Professor. Previously, 2013-2019, she was with KTH Royal Institute of

Technology in Stockholm, Sweden. Her research interests include the design of high-performance optical networks supporting next generation services, physical-layer security and reliability. She has authored over 130 publications, 8 of which received Best Paper Awards. She was a PI and WP leader of research projects funded by the EU, the Swedish Research Council, and Swedish innovation agency VINNOVA. Dr. Furdek is a Senior Member of Optica and IEEE, and was an IEEE ComSoc Distinguished Lecturer 2023-2024. She is an editor of the IEEE/Optica Journal of Optical Communications and Networking. She was a TPC Co-Chair of EuCNC & 6G Summit 2023, Chair of ECOC subcommittee SC 10 ('Control and management of optical networks') 2024-2025 and member of OFC SC N3 ('Architectures and Software-Defined Control for Metro and Core Optical Networks') 2023-2026.

ANNA TZANAKAKI

Position: Full Professor **Affiliation:** National and Kapodistrian University of Athens, Athens (Greece)

Short CV: Prof. Anna Tzanakaki is a full Professor at the National and Kapodistrian University of Athens, Greece and the Director of the MSc Programme in the fields of "Elecronics and Radioelectrology" and "Computer Automation". She has also been an adjunct faculty member of the Information Networking Institute of Carnegie Mellon University, USA. She is a co-author of over 250 publications in international journals and conferences. She is the recipient of the Jane Simons invited speaker Award (OFC 2024) and several best paper/runner up awards. She is a co-inventor of several granted and published patents. She is a member of several TPCs of international scientific conferences. She has served as an associate editor of the IEEE/OSA JOCN and is a technical referee for various conferences as well as international scientific journals. She serves and has served as a technical expert for the EU, the national research councils of Greece, UK and Portugal. She is actively participating and has participated in numerous European and national funded research collaborative projects and is currently the project and technical coordinator of the EU DEP project 5G-TACTIC.

2. Travelling Information

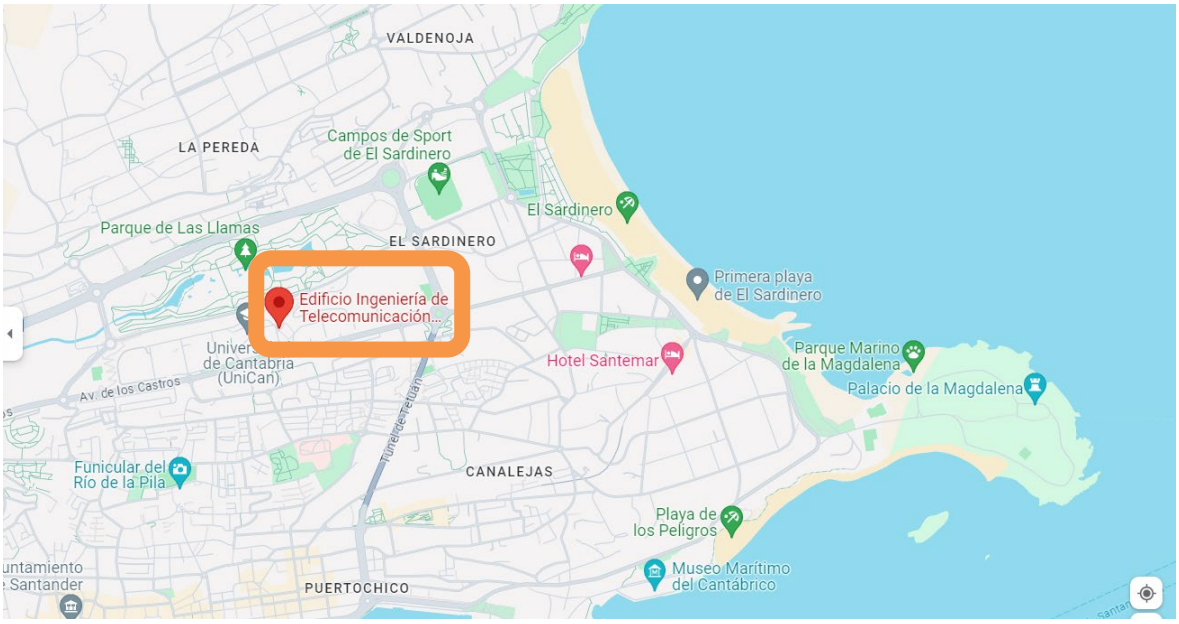
2.1. Venue

Universidad de Cantabria

Edificio de Ingeniería de Telecomunicación Prof. José Luis García.

Plaza de la Ciencia s/n, 39005, Santander, Cantabria, España

The following figures will help you reach the course venue:



Entrance to the Venue, signs will guide you through the building up to the Meeting Room

2.2. How to reach Santander

2.2.1. By Air via Santander Airport

The city airport, Seve Ballesteros-Santander (SDR), is connected (on a daily basis) with the two most important Spanish airports: Madrid-Barajas (MAD) and Barcelona-El Prat (BCN), both of which are very well connected with a large number of European cities. The duration of the domestic flight from either MAD or BCN to SDR is about one hour. In addition, Ryanair/Wizzair provides some direct, low-cost flights that connect Santander with several European Airports, namely Brussels Charleroi, Bucharest, Edimburgh and London. Please double check current timetables and offers. Once you arrive at Santander airport, the best way to reach the city is by taxi. The taxi ride should cost no more than 30€.

Additionally, there is a bus service to Santander Bus Station, located in the city center; it takes about 15 minutes and costs less than 4 €.

2.2.2. By Air via Bilbao

Santander can also be reached via Bilbao Airport (BIO), which is about 115 km from Santander (approx. 1 hour and 15-minute drive). The Bilbao Airport has direct flights to several European airports, such as Paris-Charles de Gaulle (CDG), London-Heathrow (LHR), Frankfurt-International (FRA), Brussels-National (BRU), Milan-Malpensa (MXP), Munich-FJS (MUC), and Stuttgart (STR). Other connections are also available.

From Bilbao Airport, you can reach Santander either by taking a taxi directly to Santander (cost: 120-160€), by hiring a car in the airport, or even via public transport, namely bus. In this case, there is a direct connection from the airport to the Bilbao bus station each 20 minutes, and then it is possible to take another bus from there to Santander Bus Station with Alsa bus company.

2.2.3. By Car

Santander is just off the main A8 motorway which crosses the north of Spain along the coast, the next cities being Bilbao to the East and Oviedo to the West. The A67 motorway heads south towards Torrelavega, Reinosa and Madrid beyond. Following signs on the main A8/A67 for Santander will eventually take you right into the centre of town, alongside the ferry port. Both the Ferry terminal and the Airport are clearly signposted off all motorways.

With regard to parking in Santander, there are plenty of underground car parks in the city (all charging), and there is plenty of free parking up near the Sardinero beaches. Street parking in the city centre is simple thanks to the existence of the surface regulated parking (O.L.A) where it is allowed to park in the areas marked in blue for a maximum of 2 hours. It is possible to pay through the APP or directly in the totems installed in the street.

- Monday to Friday from 10:00h to 14:00h and from 16:00h to 20:00h
- Saturdays from 10:00h to 14:00h
- Sundays and holidays without service, free parking.

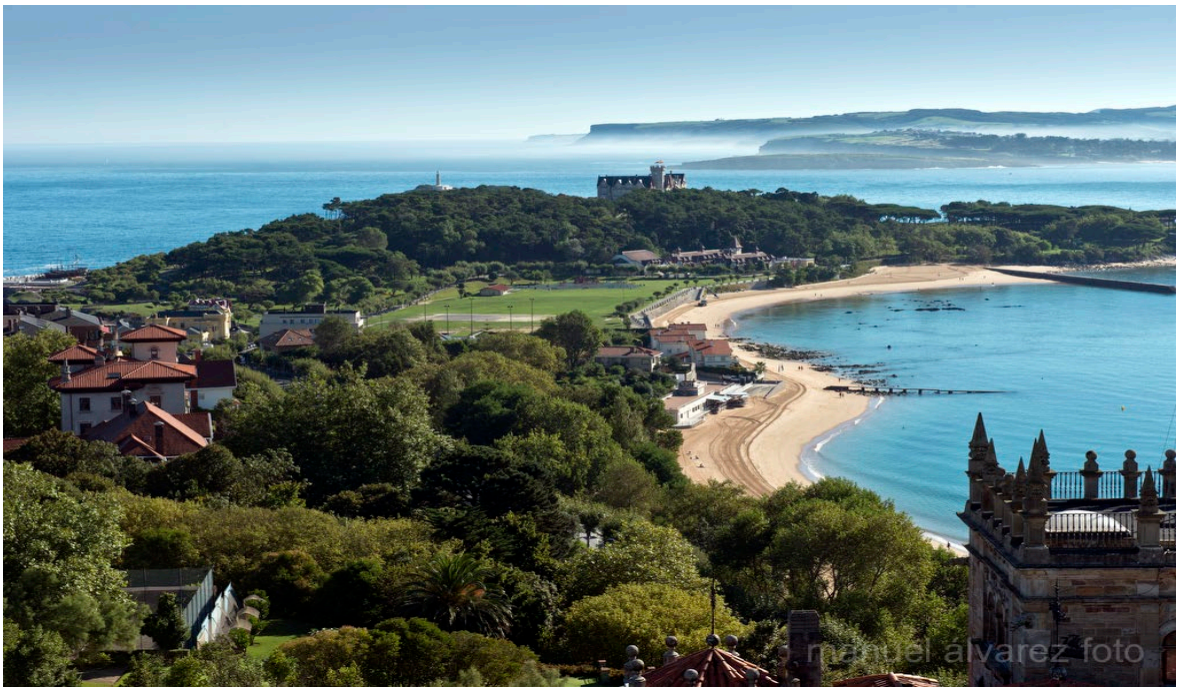
2.2.4. By Train

Santander is well served by RENFE train connections. Train station is located opposite the bus station in Santander. RENFE runs two types of services out of Santander, Long Distance trains and Cercanias (local) trains. The Long-Distance trains run twice daily to Madrid (5 and a half hours).

2.2.5. By Bus

The bus station in Santander is opposite the train stations in *Plaza Estaciones* in the centre of the city. Buses run from here all over Cantabria, Spain and beyond. The station is well equipped with information points, ticket sales, and food outlets, and buses leave from the bottom floor, with the exception of some city buses and the airport shuttle, which leave from outside the building at street level (to the left of the entrance). There is a taxi rank outside the station. For buses times to anywhere from Santander, see here, this encompasses all of the many companies which provide the services.

2.3. Welcome to Santander!



The port city of Santander is the capital of the autonomous community and historical region of Cantabria situated on the north coast of Spain. Located east of Gijón and west of Bilbao, the city has a population of aprox. 175,000 inhabitants.

The northern regions of Spain are often the less spoiled by tourism and also less know to foreign visitors, but the north of Spain keeps some of the jewels of the country: amazing landscapes and charming beaches, friendly peoples and nature preserves.

Santander is a middle-large size city that spreads along the bay. There are several beaches and harbours limiting the city on the northern side, towards the southern part you'll find the old city centre and a bit further the green mountains. We could say that Santander is between the blue and the green.

In the 19th century the city was a renowned tourist resort for Spanish politicians, aristocrats and for the upper class. The city still keeps wonderful palaces and promenades, bay type architecture with white buildings, old cafés and its famous casino.

This is undoubtedly one of the Spanish cities that you cannot miss when travelling to Spain. Santander is still an important tourism destination in Spain, especially among Spaniards themselves. Besides its appeal as a holiday resort, the city is becoming an important centre for congresses and conferences. Additionally, the whole region of Cantabria has a wide range of opportunities and excursions for exploring the nature, with beautiful mountains, prehistoric sites, sky resorts, beautiful villages and world heritage sites.

Outstanding places near Santander in the region of Cantabria are the Altamira caves with prehistoric paintings, the park of Cabárceno, the charming village of Santillana del Mar, Comillas with its University or Suances, famous for its beaches.

For further information:

https://turismo.santander.es/en/

https://turismo.santander.es/en/prepare-your-trip/useful-information/

2.4. Where to stay in Santander

Santander has a huge variety of nice hotels to stay in. We have an extensive hotel offer that you can discover by downloading the following guide on available accommodation.

As Santander is small medium city, you can choose hotels near the beach area or in the center of the city. Please, find here the one that fits your preferences best.

Additionally, there is a student hall of residence, Micampus, 15 minutes by bus from the University of Cantabria campus.

2.5. On Site support

Alberto García Email: alberto.garcia@unican.es

Luis Francisco Diez Email: luisfrancisco.diez@unican.es