****Uma imagem com Gráficos, captura de ecrã, design gráfico, texto

Descrição gerada automaticamenteA red and black logo

Description automatically generated with low confidence

B-READI

Intellectual Output - 3

DEVELOPMENT OF THE NEW MODULES FOR THE RENOVATION/INTRODUCTION OF THE DEGREES/TRACKS

Final Report

Graphical user interface, text, application

Description automatically generatedA red and black logo

Description automatically generated with low confidence **FINAL REPORT**

**INTELLECTUAL OUTPUT 3**

**DEVELOPMENT OF THE NEW MODULES FOR THE**

**RENOVATION/INTRODUCTION OF THE DEGREES/TRACKS**

Based on the work carried out in previous stages of the project, the team led by the members of the UoA executed the following tasks of the scope of the IO3:

1. Review and adjustment of the draft document containing the Competencies and the Programme Learning Outcomes (PLOs) for the European Prevention Manager (EPM) and the European Crisis Emergency Manager (ECEM) curricula.

The resulting list of PLOs, organized according to the system of pre-established competencies, was revised and corrected for clarity, with a code being assigned to each PLO.

1. Identify the existing modules of each partner institution to be included in the EPM and the ECEM curricula.

A review of the curricular contents of the programs offered at the partner institutions in the four previously identified macro areas of integrated specialist sciences - law, engineering/exact sciences, health, social sciences - (see B-READI IO1 Activities Report, p. 70), made it possible to identify the modules, or parts of them, that could meet the PLOs in the curricula to be developed.

1. Specify the module designation and its content, assessment, and learning outcomes.

A form was created for each proposed module containing information regarding its identification and implementation, namely the designation, content, teaching method to be used, evaluation and PLOs to be achieved (Appendix 1).

1. List the PLOs, with their code and description, and the modules in which they are considered, with a description of their topics, for the ECEM and EPM profiles (Tables 2 and 3).

The list also includes a reference to the partner institution that identified corresponding content in its curricula. The display allows verfying that 51,2% of EPM PLOs and 58,1% of ECEM PLOs are not covered by existing modules in the partner institutions.

The teamwork proceeded throughout ten online meeting sessions (held on Zoom), from September 2022 to February 2023, as presented in the following table (Table 1), and a session during the transnational meeting at the University of Girona, on 20 and 21 February 2023.

Table 1 – Date and Time of IO3 Team Meetings

|  |  |
| --- | --- |
| Date: | Time: |
| 23/09/2022, Friday | 09:00 – 10:00 (AZO) / 11:00 – 12:00 (CET) |
| 30/09/2022, Friday | 09:00 – 10:00 (AZO) / 11:00 – 12:00 (CET) |
| 06/10/2022, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |
| 20/10/2022, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |
| 03/11/2022, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |
| 17/11/2022, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |
| 15/12/2022, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |
| 05/01/2023, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |
| 20/01/2023, Friday | 10:00 – 11:00 AZO) / 12:00 – 13:00 (CET) |
| 09/02/2023, Thursday | 10:00 – 11:00 (AZO) / 12:00 – 13:00 (CET) |

TABLE 2 – PLOs (with code and description) and Modules (with Topic and Partner) considered for the **EPM Profile.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PLO #** | **PLO Description** | **Partner** | **Module** | **Topic** |
| **A - DEMONSTRATE AWARENESS OF RELEVANT LEGISLATION, POLICY AND LEGAL CONSTRAINTS** | | | | |
| **A1. RULES AND LEGISLATION** | | | | |
| **EPM A1.1** | Knowledge and understanding of the impact and the range of applicability of local, regional, national and European legislation | MUHEC | Digital Evidence | Law foundations in relation to forensic computing |
| **EPM A1.2** | The policies and legal constraints, related to risks management (*e.g.* labour risks, cyber risk, natural risk, *etc*.) | UNIVAQ | Cyber Security Risks and Data Protection | Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly. |
| UdG | Cyber Security Risks and Data Protection | Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly. |
| MUHEC | Fin Crime Risks from Emerging Technologies | Relevant regulatory frameworks for financial services, and the practice of regulatory compliance in corporate organizations |
| MUHEC | Open-Source Intelligence Techniques | The application of investigative guidelines, ethical practices and legislation |
| **EPM A1.3** | The legal framework that determines public policies in terms of civil protection services | UoA | Civil Protection Structures and Agents | The different organizations, structures and civil protection agents are discussed regarding the structure, organization, competences and duties. |
| EDIMAS | National and European Civil Protection | The module provides knowledge about of “European Civil Protection system” and the characteristics that this “public service” has in the Member States.  It also provides information on the European civil protection Mechanism to which European and foreign States can request support in case of need.  Particular attention is paid to the functioning and “integration of public and private functions in local, territorial, national and European governance structures. |
| MUHEC | Open-Source Intelligence Techniques | The application of investigative guidelines, ethical practices and legislation |
| **EPM A1.4** | The relevant legislation, public policies to mitigate natural and anthropic risks | UoA | Natural and Technological Risks | Integrated view of natural and technological risks. Objectives of this module: strengthening of notions and principles; and acquiring a better perception of public policies in the field of risk prevention, whether in their construction or implementation. |
| EDIMAS | National and European Civil Protection | The module provides knowledge about of “European Civil Protection system” and the characteristics that this “public service” has in the Member States.  It also provides information on the European civil protection Mechanism to which European and foreign States can request support in case of need.  Particular attention is paid to the functioning and “integration of public and private functions in local, territorial, national and European governance structures. |
| **A2. AWARENESS OF POLICY MAKERS, ENFORCING, ENACTING THESE POLICIES** | | | | |
| **EPM A2.1** | Capacity to solve possible conflicts or interference among the different level of legislation |  |  |  |
| **EPM A2.2** | Understand the structure and functioning of the crisis, emergency prevention management institutions in the country (public and private), the key actors in charge |  |  |  |
| **EPM A2.3** | Identify the legislation entities and the government departments in charge of the civil protection plans**,** the key Actors in charge |  |  |  |
| **EPM A2.4** | Identify and characterize international civil protection institutions and related organizations and structures, the key Actors in charge | UoA | Civil Protection Structures and Agents | The different organizations, structures and civil protection agents are discussed regarding the structure, organization, competences and duties. |
| **EPM A2.5** | Understand the role of the National Civil Protection Authority and national civil protection structures**,** the key Actors in charge |  |  |  |
| **EPM A2.6** | Know the key actors of civil protection system | UoA | Civil Protection Structures and Agents | The different organizations, structures and civil protection agents are discussed regarding the structure, organization, competences and duties. |
| **A3. MULTI RISK SCENARIOS OF WHICH AWARENESS SHOULD BE DEMONSTRATED** | | | | |
| **EPM A3.1** | Ability to identify and apply the proper regulations to each specific Multi Risk scenario | EDIMAS | Agenda 2030  & Emergency Management | Environment, socioeconomics, and social security (civil defence, public health, social welfare, and civil protection) are the areas of intervention of the European Emergency Management. This module addresses the immersive interconnections between the integrated strategic prevention of the UN 2030 Agenda and the innovative approach to the governance of the complexities related to crises and emergencies.  Module topics include:   * Introduction to the UN Agenda 2030. * Phases of integrated strategic planning. * information on European Prevention Management and Emergency Management. * Study cases. |
| **EPM A3.2** | Identify preventive measures to mitigate risk and recognize the difficulties inherent in their implementation | UoA | Natural and Technological Risks | Integrated view of natural and technological risks. Objectives of this module: strengthening of notions and principles; and acquiring a better perception of public policies in the field of risk prevention, whether in their construction or implementation. |
| MUHEC | Blockchain Anatomy and Analytics | Collate evidence from various sources to maintain an audit trail |
| MUHEC | Penetration Testing and Digital Forensic | Information gathering, reconnaissance and the penetration testing process |
| MUHEC | Network Security and Services | Security threats and the available security mechanisms for combating security breaches |
| MUHEC | Cyber Security and Legal Regulations | Risk Assessment Process |
| **EPM A3.3** | Know, understand and adopt the key governance aspects and resources available for an integrated strategic multidisciplinary territorial planning for risk prevention, shared with key Actors of the civil protection system | MUHEC | Risk Management Principles (no module code) | Risk management frameworks and governance concepts (IRGC and ISO guidance) |
| **A4. CRITICAL THINKING AND PROBLEM SOLVING** | | | | |
| **EPM A4.1** | Critically reflect on the impact of relevant legislation and policies for Integrated Strategic Multidisciplinary Territorial Planning for Risk Prevention | UNIVAQ | Cyber Security Risks and Data Protection | Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly. |
| UdG | Cyber Security Risks and Data Protection | Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly. |
| MUHEC | Digital Evidence | Computer related crime / Sources of legal information |
| **B - DEMONSTRATE SUFFICIENT AWARENESS OF RELEVANT ENGINEERING APPROACHES AND RELATED PROBLEM-SOLVING SKILLS** | | | | |
| **B1. RISK ANALYSIS AND ASSESSMENT** | | | | |
| **EPM B1.1** | Recognize the importance of timely dissemination of information (UoA) | UoA | Monitoring and Warning Systems | Monitoring and Early Warning Systems are essential for the mitigation of hazards. The module addresses the implementation of a warning system according to the type of hazards to be monitored and the necessary resources for that purpose. It also explains how the information is generated, transformed into warning messages, and disseminated using resources to the various communication systems |
| **EPM B1.2** | Ability to identify and rank the main crisis events with high occurrence probability in the territory of reference in order to select the most suitable engineering approaches (UnivAQ) | UnivAQ | ? | ? |
| **EPM B1.3** | Capacity to identify the problems and provide the correct solutions through an integrated multidisciplinary preventionplan (UnivAQ) | MUHEC | Blockchain Anatomy and Analytics | Deploy appropriate tools and techniques to carry out an investigation |
| MUHEC | Digital Forensics & Incident Management | Procedures of examining digital evidence collection and seizure with the possible limitations in the context of constantly changing technologies |
| MUHEC | Fin Crime Risks from Emerging Technologies | Changing financial crime typologies from new emerging technologies |
| MUHEC | Open-Source Intelligence Techniques | Evaluate open-source data gathering intelligence techniques and collection methodologies |
| MUHEC | Penetration Testing and Digital Forensic | Identify and solve problems, both individually and working in groups |
| MUHEC | Network Security and Services | Design and implementation of security mechanisms for a given network |
| MUHEC | Cyber Security and Legal Regulations | Incident response planning |
| MUHEC | Risk Management Principles (no module code) | Social impacts and vulnerability to flooding (western Europe) |
| **EMP B1.4** | Knowledge of the risk levels and capacity to describe coherently the scenario in terms of prevention and engineering actions. Knowledge of software risk assessment tools (UdG) |  |  |  |
| **B2. PREVENTION FOR RISK REDUCTION/ MITIGATION INTEGRATED STRATEGIC MULTIDISCIPLINARY TERRITORIAL PLANNING** | | | | |
| **EPM B2.1** | Identify the coordination methodology processes and tools**,** according to the selected prevention plans | UNIVAQ | Cyber Security Risks and Data Protection | Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly. |
| UdG | Cyber Security Risks and Data Protection | Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly. |
| MUHEC | Blockchain Anatomy and Analytics | Techniques to identify suspects |
| MUHEC | Digital Forensics & Incident Management | Procedures and models for establishing and maintaining a physical "chain of custody” and critically evaluate their effectiveness in a variety of digital crime scenarios |
| MUHEC | Fin Crime Risks from Emerging Technologies | New technologies for vulnerability to financial crime and develop prevention strategies |
| MUHEC | Open-Source Intelligence Techniques | Various techniques for advanced searching and data gathering methods |
| MUHEC | Penetration Testing and Digital Forensic | Formulate appropriate methods for troubleshooting |
| MUHEC | Network Security and Services | Security policies, services and mechanisms |
| MUHEC | Cyber Security and Legal Regulations | Security programs, policies, procedures, standards and guidelines |
| MUHEC | Risk Management Principles (no module code) | Introducing flood warning and emergency response |
| **EPM B2.2** | Knowledge of and capacity to properly use the main tools | UNIVAQ | Data Acquisition and Visualization (University of L’Aquila) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| UdG | Data Acquisition and Visualization (UdG) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| MUHEC | Blockchain Anatomy and Analytics | Measures to facilitate seizure |
| MUHEC | Digital Forensics & Incident Management | Appropriate tools to carry out digital forensics search and seizure independently and as part of a team |
| MUHEC | Fin Crime Risks from Emerging Technologies | Reg Tech: the use of technology to address financial crime risk |
| MUHEC | Open-Source Intelligence Techniques | Various techniques for advanced searching and data gathering methods |
| MUHEC | Penetration Testing and Digital Forensic | Design and plan a penetration test in accordance with current standards and legal / ethical issues |
| MUHEC | Network Security and Services | Hardware and software security applications |
| MUHEC | Cyber Security and Legal Regulations | Prepare and test plans for contingencies and disasters |
| MUHEC | Risk Management Principles (no module code) | Introducing flood warning and emergency response |
| **B3. MONITORING AND EWS (EARLY-WARNING SYSTEMS)** | | | | |
| **EPM B3.1** | Recognize and understand the importance of the role played by monitoring and EWS | UNIVAQ | Data Acquisition and Visualization (University of L’Aquila) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| UdG | Data Acquisition and Visualization (UdG) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| **EPM B3.2** | Recognize and understand the main elements that govern the design of EWS | UoA | Monitoring and Warning Systems | Monitoring and Early Warning Systems are essential for the mitigation of hazards. The module addresses the implementation of a warning system according to the type of hazards to be monitored and the necessary resources for that purpose. It also explains how the information is generated, transformed into warning messages, and disseminated using resources to the various communication systems |
| UNIVAQ | Data Acquisition and Visualization (University of L’Aquila) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| UdG | Data Acquisition and Visualization (UdG) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| **EPM B3.3** | Know the involvement of intergovernmental organizations in monitoring and alert systems |  |  |  |
| **EPM B3.4** | Know the different types of monitoring systems used in theforecast of natural and technological phenomena |  |  |  |
| **EPM B3.5** | Recognize and understand the variety and complexity of existing monitoring and EWS “Early Warning Systems” and their use in a multi-hazard perspective | UoA | Monitoring and Warning Systems | Monitoring and Early Warning Systems are essential for the mitigation of hazards. The module addresses the implementation of a warning system according to the type of hazards to be monitored and the necessary resources for that purpose. It also explains how the information is generated, transformed into warning messages, and disseminated using resources to the various communication systems |
| UNIVAQ | Data Acquisition and Visualization (University of L’Aquila) | In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis. Also, these data must be adequately presented in order to help in the decision-making process.  The goal of this course is to provide the motivations, definitions and techniques for the acquisition and manipulation of data coming from the systems of smart buildings and facilities in a smart city |
| **EPM B3.6** | Know and understand the different monitoring and Early Warning Systems applied in order to reduce/mitigate natural, anthropic and modern risks | UoA | Monitoring and Warning Systems | Monitoring and Early Warning Systems are essential for the mitigation of hazards. The module addresses the implementation of a warning system according to the type of hazards to be monitored and the necessary resources for that purpose. It also explains how the information is generated, transformed into warning messages, and disseminated using resources to the various communication systems |
| MUHEC | Risk Management Principles (no module code) | Introducing flood warning and emergency response |
| **B4. SYSTEMIC AND INTERDISCIPLINARY APPROACH TO REDUCTION/MITIGATION OF RISK** | | | | |
| **EPM B4.1** | Demonstratemanagerial skills of the actor in charge to coordinate multiple professional activities in possible risk scenarios in the Local Managing Authority | MUHEC | Digital Evidence | Investigation techniques |
| **EPM B4.2** | Knowledge and understanding of the requiredSystemic and interdisciplinary approach in reduction/mitigation of Risk | MUHEC | Blockchain Anatomy and Analytics | Blockchain artefacts in the context of a digital investigation of cryptocurrencies and crime |
| MUHEC | Digital Forensics & Incident Management | Maintain a comprehensive audit trail for the production of reports and statements to be used in a court of law |
| MUHEC | Fin Crime Risks from Emerging Technologies | Future readiness strategy development |
| MUHEC | Open-Source Intelligence Techniques | The application of investigative guidelines, ethical practices and legislation |
| MUHEC | Penetration Testing and Digital Forensic | Evaluate the design of countermeasures for computer and network flaws found as a result of penetration tests |
| MUHEC | Network Security and Services | Security policies, services and mechanisms |
| MUHEC | Cyber Security and Legal Regulations | Assess and manage risk in enterprise systems and networks |
| **EPM B4.3** | Problem solving skills required in systemic and interdisciplinary approaches for reduction/mitigation of risk | MUHEC | Blockchain Anatomy and Analytics | Application of open-source investigation techniques in cryptocurrency and blockchain investigations |
| MUHEC | Digital Forensics & Incident Management | Investigative guidelines for digital investigations |
| MUHEC | Fin Crime Risks from Emerging Technologies | Impact assessment of new technologies in practice |
| MUHEC | Open-Source Intelligence Techniques | Advanced techniques to gather intelligence and evidence |
| MUHEC | Penetration Testing and Digital Forensic | Evaluate the design of countermeasures for computer and network flaws found as a result of penetration tests |
| MUHEC | Network Security and Services | Solutions for real world current and future security threats, including the implementation of innovative solutions |
| MUHEC | Cyber Security and Legal Regulations | Framework for cyber security and industrial IT |
| MUHEC | Digital Evidence | Investigation techniques |
| **C - DEMONSTRATE AWARENESS AND APPRECIATION OF THE HEALTH SYSTEM AND PROVIDED SERVICES** | | | | |
| **C1. HEALTH ASPECTS IN THE TERRITORIAL MULTIDISCIPLINARY STRATEGIC INTEGRATED PLANNING ACTIVITY FOR RISK PREVENTION (MULTI-RISK)** | | | | |
| **EPM C1.1** | Knowledge and understanding of the multilevel responsibilities of health systems (including the social services, ambulance services, vets, etc.) and their relations with the strategical territorial planning | ? | ? |  |
| **EPM C1.2** | Capacity to imagine the risk scenarios, in order to cope with any problem even those with low probability to incur (residual risks) providing a quick response in the framework of a proper integrated strategic plan | ? | ? |  |
| **EPM C1.3** | Demonstrate the multilevel responsibilities associated with health aspects in Integrated Strategic prevention | UdG | Psychological Intervention in Emergency Crisis (Universitat de Girona) | It is important for the emergency professionals to consider and evaluate the psychological status of the victims to predict their reactions. Basic notions are necessary for stablishing a good communication with the victims and give a first basic psychological intervention in contexts of emergencies or disasters. |
| **C2. HEALTH SYSTEMS – STRUCTURES AND ORGANIZATIONS, KNOWLEDGE AND COORDINATION (EPM)** | | | | |
| **EPM C2.1** | Identify and coordinate the health services and professionals involved in a specific prevention plan area | UdG | Psychological Intervention in Emergency Crisis (Universitat de Girona) | It is important for the emergency professionals to consider and evaluate the psychological status of the victims to predict their reactions. Basic notions are necessary for stablishing a good communication with the victims and give a first basic psychological intervention in contexts of emergencies or disasters. |
| **EPM C2.2** | Demonstrate knowledge and understanding of the medical skills required inPrevention Planning against Risk scenarios. | UdG | Psychological Intervention in Emergency Crisis (Universitat de Girona) | It is important for the emergency professionals to consider and evaluate the psychological status of the victims to predict their reactions. Basic notions are necessary for stablishing a good communication with the victims and give a first basic psychological intervention in contexts of emergencies or disasters. |
| **D - DEMONSTRATE THE ABILITY TO MANAGE MULTIDISCIPLINARY TEAMS IN PREVENTION PLANNING OF RISK SCENARIOS** | | | | |
| **D1. EMERGENCY MANAGEMENT CYCLE** | | | | |
| **EPM D1.1** | Capacity to identify the prevention plan/s referred to Major Events and related Risks | **EDIMAS** | Agenda 2030 & Emergency Management | Environment, socioeconomics, and social security (civil defence, public health, social welfare, and civil protection) are the areas of intervention of the European Emergency Management. This module addresses the immersive interconnections between the integrated strategic prevention of the UN 2030 Agenda and the innovative approach to the governance of the complexities related to crises and emergencies.  Module topics include:   * Introduction to the UN Agenda 2030. * Phases of integrated strategic planning. * information on European Prevention Management and Emergency Management. * Study cases. |
| **EPM D1.2** | Identification of the rules to improve the plan strategies in future actions | MUHEC | Risk Management Principles (no module code) | Preventative health and safety. |
| MUHEC | Risk Management Principles (no module code) | Risk assessment challenges. |
| MUHEC | Risk Management Principles (no module code) | Tolerability of risk including frameworks and concepts such a ALARP/ALARA. |
| MUHEC | Risk Management Principles (no module code) | Built environment risk management. |
| **EPM D1.3** | Recognize the close link among the different phases of risk prevention management | UoA | Crisis Management and Response Mechanisms | Facts that contribute to the complexity of crisis management in the different phases of disaster management |
| MUHEC | Risk Management Principles (no module code) | Risk communication (perception, world views, values, biases) |
| **D2. SCENARIO-BASED RESPONSE PLANNING** | | | | |
| **EPM D2.1** | Capacity to describe the prevention activities, in each identified predictable scenario, providing a list of solutions to any foreseen problem |  |  |  |
| **EPM D2.2** | Knowledge and understanding of the factors including approaches and skills that condition the success of crisis/emergency management (Planning) (UoA) | UoA | Crisis Management and Response Mechanisms | Facts that contribute to the complexity of crisis management in the different phases of disaster management |
| MUHEC | Risk Management Principles (no module code) | Business continuity |
| **D3. ACTORS AND ROLES IN PREVENTION PLANNING OF CRISIS AND EMERGENCY MANAGEMENT** | | | | |
| **EPM D3.1** | Knowledge and understanding of the bodies in charge to operate in the territory in case of Crisis/Emergency Scenarios (Planning) | UdG | Psychological Intervention in Emergency Crisis (Universitat de Girona) | It is important for the emergency professionals to consider and evaluate the psychological status of the victims to predict their reactions. Basic notions are necessary for stablishing a good communication with the victims and give a first basic psychological intervention in contexts of emergencies or disasters. |
| **D4. LEADERSHIP STYLE AND CAPACITY IN MANAGING A MULTIDISCIPLINARY TEAM (PUBLIC AND PRIVATE)** | | | | |
| **EPM D4.1** | Ability to assign the right task to each body avoiding overlapping and time wasting |  |  |  |
| **EPM D4.2** | Knowledge and understanding (in planning) of the involved tools to coordinate the different bodies (public and private) | MUHEC | Digital Evidence | E-Crime detection / Crime interception |
| MUHEC | Risk Management Principles (no module code) | Stakeholder engagement and planning |

TABLE 3 – PLOs (with code and description) and Modules (with Topic and Partner) considered for the **ECEM profile.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PLO #** | **PLO Description** | **Partner** | **Module** | **Topic** |
| **A - DEMONSTRATE AN EXHAUSTIVE AWARENESS OF LEGISLATION, POLICIES AND LEGAL CONSTRAINTS RELEVANT TO THE GOVERNANCE OF CRISIS AND EMERGENCY MANAGEMENT (SPECIFIC RESPONSIBILITIES OF INDIVIDUAL LOCAL, REGIONAL AND NATIONAL AUTHORITIES)** | | | | |
| **A1. RULES AND LEGISLATION. KNOWLEDGE AND ANALYSIS OF EXISTING LEGAL/REGULATORY FRAMEWORKS** | | | | |
| **ECEM A1.1** | Identify the encountered/possible gaps in the present legislation and suggest the solution and the consequent needed amendments, referring to different governance levels | ? | ? | ? |
| **ECEM A1.2** | Analyse and evaluate the present rules concerning the tasks and roles of each body in charge of crisis governance and emergency management | EDIMAS | National and European  Civil Protection | The training module provides knowledge of the "European civil protection system" and of the characteristics that this "public service" has in the Member States. Particular attention is paid to:  - the activation processes of the European Civil Protection Mechanism when a European State or a foreign State makes a request for support.  - the functioning and activation of the "Operational Modules" of the European Civil Protection Mechanism |
| **ECEM A1.3** | Assess the actual legal constraints faced by a crisis/emergency manager | MUHEC | Open-Source Intelligence Techniques | Application of investigative guidelines, ethical practices and legislation |
| **ECEM A1.4** | Specify knowledge of the current policies and regulations related to risks in crisis management (e.g. labour risks, cyber-attacks, natural disasters, etc.) | ? | ? | ? |
| **ECEM A1.5** | Know public policies to reduce natural and anthropic risks in crisis management | UoA | Natural and Technological Risks | Integrated view of natural and technological risks. Objectives of this module: strengthening of notions and principles; and acquiring a better perception of public policies in the field of risk prevention, whether in their construction or implementation. |
| EDIMAS | National and European  Civil Protection | The training module provides knowledge of the "European civil protection system" and of the characteristics that this "public service" has in the Member States. Particular attention is paid to:  - the activation processes of the European Civil Protection Mechanism when a European State or a foreign State makes a request for support.  - the functioning and activation of the "Operational Modules" of the European Civil Protection Mechanism |
| **ECEM A1.6** | Critically reflect on the impact of relevant legislation and policies upon integrated emergency response | MUHEC | Digital Evidence | Law foundations in relation to forensic computing |
| **ECEM A1.7** | Determine and understand the key governance aspects and resources available in an emergency | MUHEC | Digital Evidence | The role of the computer forensic professional |
| **A2. AWARENESS OF LOCAL, REGIONAL AND NATIONAL STAKEHOLDERS/ACTORS** | | | | |
| **ECEM A2.1** | Understand the structure and functioning of the emergency management institutions in the country (public and private), stakeholders/actors | ? | ? | ? |
| **ECEM A2.2** | Identify and characterise international civil protection organizations and structures (UoA). | UoA | Civil Protection Structures and Agents | The different organizations, structures and civil protection agents are discussed regarding the structure, organization, competences and duties. |
| **A3. RISKS MITIGATION STRATEGIES IN CRISIS MANAGEMENT** | | | | |
| **ECEM A3.1** | Understand the level of complexity in the risk assessment processes for the best emergency planning (UoA) | UoA | Natural and Technological Risks | Integrated view of natural and technological risks. Objectives of this module: strengthening of notions and principles; and acquiring a better perception of public policies in the field of risk prevention, whether in their construction or implementation. |
| MUHEC | Digital Forensics  & Incident Management | Documentation, reporting and analysis of digital e-crimes using case scenarios |
| MUHEC | Fin Crime Risks from Emerging Technologies: | Policy documents and to give advice on matters regarding compliance and crime from new emerging technologies |
| MUHEC | Penetration Testing and Digital Forensic: | Apply relevant theoretical concepts to Identify and solve problems |
| MUHEC | Network Security and Services: | Security threats and the available security mechanisms for combating security breaches |
| MUHEC | Cyber Security and Legal Regulations: | Risk Assessment Process |
| **ECEM A3.2** | Identify measures to reduce/mitigate risk in crisis management and recognize the difficulties inherent in their implementation (UoA) | UoA | Natural and Technological Risks | Integrated view of natural and technological risks. Objectives of this module: strengthening of notions and principles; and acquiring a better perception of public policies in the field of risk prevention, whether in their construction or implementation. |
| **ECEM A3.3** | Understand the range of responsibilities and interdependencies associated with crisis/emergency management (MUHEC) | MUHEC | Digital Evidence | Incidence handling |
| **B - DEMONSTRATE AN EXHAUSTIVE MANAGERIAL COMPETENCE, LEADERSHIP AND PROBLEM-SOLVING SKILLS FOR THE COORDINATION OF THE COMPONENTS AND OPERATIONAL STRUCTURES OF CIVIL DEFENCE (\*), CIVIL PROTECTION AND PUBLIC HEALTH BODIES ACCORDING TO THE EVENT SCENARIO (FIREFIGHTERS, LAW ENFORCEMENT AND MILITARY, HEALTH CARE AND CIVIL PROTECTION VOLUNTEERS)** | | | | |
| **B1. “THREAT ASSESSMENT” AND “RISK ANALYSIS AND ASSESSMENT” IN “CRISIS EVENT MANAGEMENT”** | | | | |
| **ECEM B1.1** | Identify and select the suitable tools (such as digital tools and non-digital tools) in crisis event management (UdG) | MUHEC | Blockchain Anatomy and Analytics | Cryptocurrency / blockchain visualization and analytics |
| MUHEC | Digital Forensics & Incident Management | Appropriate tools to carry out digital forensics search and seizure independently and as part of a team |
| MUHEC | Fin Crime Risks from Emerging Technologies | New technologies for vulnerability to financial crime and develop prevention strategies |
| MUHEC | Open-Source Intelligence Techniques | Open-source data gathering intelligence techniques and collection methodologies |
| MUHEC | Penetration Testing and Digital Forensic | Attack tools, application usage and development, including writing exploits and payloads |
| MUHEC | Network Security and Services | Authentication and authorisation, intrusion detection and information security techniques |
| MUHEC | Cyber Security and Legal Regulations | Disaster recovery planning |
| **ECEM B1.2** | Recognize the importance of timely and competentinformation to the citizens (UoA) | UoA | Monitoring and Warning Systems | Monitoring and Early Warning Systems are essential for the mitigation of hazards. The module addresses the implementation of a warning system according to the type of hazards to be monitored and the necessary resources for that purpose. It also explains how the information is generated, transformed into warning messages, and disseminated using resources to the various communication systems |
| **B2. MONITORING AND WARNING SYSTEMS IN CRISIS EMERGENCY SCENARIO** | | | | |
| **ECEM B2.1** | Recognize the importance of the role played by “monitoring systems” | MUHEC | Risk Management Principles (no module code) | Flood defence approach, monitoring for maintenance UK |
| **ECEM B2.2** | Know the involvement of governance organizations in monitoring and early warning system | MUHEC | Risk Management Principles (no module code) | Introducing flood warning and emergency response |
| **B3. THE APPLICATION PROCESS OF THE CRISIS/EMERGENCY MANAGEMENT PLANNING** | | | | |
| **ECEM B3.1** | Capacity to identify risk levels and to describe and cope with the scenario in terms of crisis/emergency management and multifunctional actions | MUHEC | Blockchain Anatomy and Analytics | Techniques to identify suspects |
| MUHEC | Digital Forensics & Incident Management | Forensic environment requirements |
| MUHEC | Fin Crime Risks from Emerging Technologies | Financial crime concepts and types of crime |
| MUHEC | Open-Source Intelligence Techniques | Various techniques for advanced searching and data gathering methods |
| MUHEC | Penetration Testing and Digital Forensic | Evaluate research and different types of information & evidence arguments critically |
| MUHEC | Network Security and Services | Technical security systems |
| MUHEC | Cyber Security and Legal Regulations | Prepare and test plans for contingencies and disasters |
| **ECEM B3.2** | Evaluate the technicalskills and identify the missing ones for a suitable crisis management | MUHEC | Fin Crime Risks from Emerging Technologies | Opportunities and vulnerabilities of adopting emerging technology for business |
| MUHEC | Network Security and Services | Security mechanisms for a given network |
| MUHEC | Cyber Security and Legal Regulations | Design awareness, training and education programs |
| **ECEM B3.3** | Capacity to describe the scenario and identify risk levels in relation to engineering actions and pertinent prevention measures | MUHEC | Blockchain Anatomy and Analytics | Measures to facilitate seizure |
| MUHEC | Digital Forensics & Incident Management | Incident response methodology |
| MUHEC | Open-Source Intelligence Techniques | Appropriate tools (open source and specialist tools) to carry out open-source intelligence gathering |
| MUHEC | Penetration Testing and Digital Forensic | Apply relevant theoretical concepts to Identify and solve problems |
| MUHEC | Network Security and Services | Security policies, services and mechanisms |
| MUHEC | Cyber Security and Legal Regulations | Identify common threats to applications, systems and networks |
| **ECEM B3.4** | Develop “emergency management plans” for the coordination of different operational structures required for a range of event scenarios | MUHEC | Blockchain Anatomy and Analytics | Appraise the developments in criminal techniques within domain |
| MUHEC | Digital Forensics & Incident Management | Information hiding techniques, detection and solutions |
| MUHEC | FinCrime Risks from Emerging Technologies | Understanding regulation of financial services |
| MUHEC | Open-Source Intelligence Techniques | Evaluate data sources and understand their limitations |
| MUHEC | Penetration Testing and Digital Forensic | Design and plan a penetration test in accordance with current standards |
| MUHEC | Network Security and Services | Solutions for real world current and future security threats, including the implementation of innovative solutions |
| MUHEC | Cyber Security and Legal Regulations | Assess and manage risk in enterprise systems and networks. |
| **B4. AWARENESS OF BODIES, SKILLS, COMPETENCIES AND COORDINATION INVOLVED** | | | | |
| **ECEM B4.1** | Demonstrate understanding of the range of approaches and skills required for different event scenarios. | ? | ? | ? |
| **C - DEMONSTRATE EXHAUSTIVE AWARENESS AND KNOWLEDGE OF HEALTH SYSTEM, SPECIALTIES AND RESPONSIBILITIES IN ORDER TO ENSURE A PROPER PUBLIC HEALTH INTERVENTION IN CRITICAL SCENARIOS** | | | | |
| **C1. ROLES AND COMPETENCES IN PUBLIC HEALTH SERVICES IN CRISIS/EMERGENCY SITUATIONS MANAGEMENT** | | | | |
| **ECEM C1.1** | Clear knowledge of the needed direct intervention as well as of the indirect effects on the crisis scenario management | ? | ? | ? |
| **ECEM C1.2** | Demonstrate knowledge of the health skills required in critical scenarios | UNIVAQ | Integrated Health Emergencies | TOPICS OF THE MODULE INCLUDE:  a) Emergency Medicine, Disaster Medicine and Public Health  b) Definition of emergency and disaster medicine  c) Modeling medical disaster management  d) Disaster epidemiology  e) General Medical Disaster Management  f) Specific Medical Disaster Management |
| **ECEM C1.3** | Demonstrate in depth understanding of the role of each health system unit in crisis scenario | UNIVAQ | Integrated Health Emergencies | TOPICS OF THE MODULE INCLUDE:  a) Emergency Medicine, Disaster Medicine and Public Health  b) Definition of emergency and disaster medicine  c) Modeling medical disaster management  d) Disaster epidemiology  e) General Medical Disaster Management  f) Specific Medical Disaster Management |
| **C2. TEAM COORDINATION AND MANAGEMENT IN AN EMERGENCY SITUATION ASSOCIATED WITH HEALTH ASPECTS** | | | | |
| **ECEM C2.1** | Knowledge and ability to coordinate the medical entities (public and private) in an emergency scenario | UNIVAQ | INTEGRATED HEALTH EMERGENCIES | TOPICS OF THE MODULE INCLUDE: a) Emergency Medicine, Disaster Medicine and Public Health  b) Definition of emergency and disaster medicine  c) Modeling medical disaster management  d) Disaster epidemiology  e) General Medical Disaster Management f) Specific Medical Disaster Management |
| **D - DEMONSTRATE PRACTICAL SKILLS FOR A CONCRETE INTERVENTION DIRECTLY ON THE FIELD BY USING PROPER TECHNOLOGIES AND METHODOLOGIES** | | | | |
| **D1. PHASES OF THE EUROPEAN EMERGENCY MANAGEMENT CYCLE** | | | | |
| **ECEM D1.1** | Capacity to execute an emergency management plan |  |  |  |
| **ECEM D1.2** | Recognize the close link among the different phases of emergency management | UoA | Crisis Management and Response Mechanisms | Facts that contribute to the complexity of crisis management in the different phases of disaster management |
| **ECEM D1.3** | Understand the factors that condition the success of crisis/emergency management | UoA | Crisis Management and Response Mechanisms | Facts that contribute to the complexity of crisis management in the different phases of disaster management |
| **D2. UNDERSTANDING, ASSESSING AND ASSIGNING ACTORS, ROLES AND SKILLS TO FORESEEN TASKS** | | | | |
| **ECEM D2.1** | Describe the structure and roles of a multi-disciplinary team that is formed to manage crisis/emergencies | EDIMAS | The Communication | The module offers the ability to differentiate the tools and methods of communication strategies according to the different targets:  - recipients affected by the event,  - average,  - experts,  - institutions. |
| **ECEM D2.2** | Identify the roles and responsibilities of the different crisis management teams | ? | ? | ? |
| **ECEM D2.3** | Identify the different skills needed for managing a multi-disciplinary team according to the specific crisis scenario | MUHEC | Digital Evidence | Incidence handling |
| **D3. SELECTING APPROPRIATE CRITERIA, METHODS, PROCEDURES, TOOLS, RESOURCES MULTIDISCIPLINARY AND TECHNOLOGIES IN AN EMERGENCY/CRISIS COMPLEX SCENARIOS, TAKING INTO THE DUE ACCOUNT OF OTHER RESOURCES AND METHODS THAT ARE ALSO OF DIFFERENT NATURE** | | | | |
| **ECEM D3.1** | Critically evaluate the importance of different methods and technologies available for the management of critical scenarios (\*) (MUHEC) | MUHEC | Blockchain Anatomy and Analytics | Deploy appropriate tools and techniques to carry out an investigation |
| MUHEC | Digital Forensics & Incident Management | Techniques and valid procedures to carry out digital forensic investigations on current and emerging technologies |
| MUHEC | Fin Crime Risks from Emerging Technologies | Assessment of new technologies |
| MUHEC | Open-Source Intelligence Techniques | Apply advanced techniques to gather intelligence and evidence |
| MUHEC | Penetration Testing and Digital Forensic | Systematically and critically evaluate the design of countermeasures for computer and network flaws found as a result of penetration tests |
| MUHEC | Network Security and Services | Security policies, services and mechanisms |
| MUHEC | Cyber Security and Legal Regulations | Develop security programs, policies, procedures, standards, and guidelines appropriate for corporate environments |
| MUHEC | Digital Evidence | Evidence presentation |

APPENDIX 1

**Integrated Health Emergencies (University of L’Aquila)**

|  |
| --- |
| **Pre-requisites** |
| Knowledge of Medicine, First Aid and Intensive Care. |
| **Description & Contents** |
| The course aims to train participants to deal with medical-assistance problems relating to health emergencies in the intra and extra-hospital environment.  The didactic and training plan is aimed at qualifying:   * in the knowledge of the problems related to the environment and natural disasters * in the knowledge of the physiological and pathophysiological problems of the organism in difficult * in the management of health emergencies in a hostile environment * in the use of monitoring and therapy systems already at the accident site * in the management of the patient * in the communication with the patient and with the media * in the new technologies and techniques at the service of emergencies * in the knowledge of the new technologies applicable to the emergency / max emergency |
| **Activities & Methodology** |
| Expositive sessions.  Presentation of class works (e.g. poster session, slide show, …)  Practices |
| **Evaluation / Assessment** |
| Class works 45% Practices 55% |
| **Learning outputs (Competences)** |
| **ECEM C1.2** Demonstrate knowledge of the health skills required in critical scenarios  **ECEM C1.3** Demonstrate in depth understanding of the role of each health system unit in crisis scenario  **ECEM C2.1** Knowledge and ability to coordinate the medical entities (public and private) in an emergency scenario |

**Data Acquisition and Visualization (Universitat de Girona/University of L’Aquila))**

|  |
| --- |
| **Pre-requisites** |
| Basic knowledge of computer programming. |
| **Description & Contents** |
| In emergency prevention and management scenarios there will be received data from sensors, geolocalization of equipment and personnel, etc. These could represent huge volumes of information, in some cases raw data that can be incomplete or containing errors. These data must be prepared for its analysis.  Also, these data must be adequately presented in order to help in the decision-making process.   * Sources of Data in emergencies and its acquisition * Data Quality Evaluation * Data cleansing * Data preparation for their use in Data Science * Introduction to the visualization of information. * Types of graphics and visualization strategies. * Advanced and interactive visualization |
| **Activities & Methodology** |
| Expositive sessions.  Presentation of class works (e.g. poster session, slide show, …)  Practices (development of a small project) |
| **Evaluation / Assessment** |
| Class works 35% Practices 65% |
| **Learning outputs (Competences)** |
| **EPM B2.2 -** Knowledge of and capacity to properly use the main tools  **EPM B3.1 -** Recognize and understand the importance of the role played by monitoring and EWS  **EPM B3.2 -** Recognize and understand the main elements that govern the design of EWS  **EPM B3.5 -** Recognize and understand the variety and complexity of existing monitoring and EWS “Early Warning Systems” and their use in a multi-hazard perspective |

**Cyber Security Risks and Data Protection (Universitat de Girona)**

|  |
| --- |
| **Pre-requisites** |
| Basic knowledge of computer programming, and computer networks. |
| **Description & Contents** |
| Most of the modern services and infrastructures (telecommunications, energy, water supply, transportation, etc) rely on electronic and computer systems which can be attacked. It is of major importance to maintain these services working properly.   * Introduction to cryptography * Security in Data Bases and Operating Systems * Security in Networks and Internet Services * Security in Sensors and Data Acquisition * Application of Blockchain solutions and Smart Contracts |
| **Activities & Methodology** |
| Expositive sessions.  Presentation of class works (e.g. poster sessions, slide show, etc)  Practices (programming, analyzing, etc) |
| **Evaluation / Assessment** |
| Class works 40% Practices 60% |
| **Learning outputs (Competences)** |
| **EPM B2.1 -** Identify the coordination methodology processes and tools**,** according to the selected prevention plans (UdG)  **EPM A1.2 -** The policies and legal constrains, related to risks management (e.g. labour risks, cyber risk, natural risk, etc.)  **EPM A4.1 -** Critically reflect on the impact of relevant legislation and policies for Integrated Strategic Multidisciplinary Territorial Planning for Risk Prevention |

**Monitoring and Warning Systems (University of the Azores)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| Monitoring and Early Warning Systems are essential for the mitigation of hazards. The module addresses the implementation of a warning system according to the type of hazards to be monitored and the necessary resources for that purpose. It also explains how the information is generated, transformed into warning messages, and disseminated using resources to the various communication systems.  Topics of the module include:   * Identification of natural hazards * Introduction to monitoring and warning systems * Monitoring methods and strategies * Data acquisition and transmission * Monitoring systems (*i.e.*, Gas emissions – CO2 (discrete and continuous measurements) and radon (222Rn); Water analysis – Physical and chemical parameters measured in situ and in the laboratory; Seismic monitoring; (\*) Visit to seismic stations and epicenter calculations. Geodetic landslide monitoring – using a total station method.) * Warning systems. (*i.e.,* (\*)Visit to the landslide early warning system   array of meteorological stations.)   * Communication of information warning systems to authorities, organizations, and the population |
| **Activities & Methodology** |
| Expositive sessions (oral presentation of topics using slides, illustrative diagrams, photographs, videos, etc).  Practices (development of a small project and (\*)observation of data acquisition centers and transmission systems.  (\*) Activities to be held in São Miguel Island, Azores |
| **Evaluation / Assessment** |
| Class works 40% Practices 60% |
| **Learning outputs (Competences)** |
| **EPM B1.1 -** Recognize the importance of timely dissemination of information (UoA)  ECEM B1.2 - Recognize the importance of timely and competent information to the citizens (UoA)  EPM B3.2 - Understand the main elements that govern the design of an early warning system (UoA)  EPM B3.5 - Recognize and understand the variety and complexity of existing monitoring and early warning systems and their use in a multi-hazard perspective (UoA)  EPM B3.6 - Know and understand the different monitoring and early warning systems applied in order to reduce / mitigate natural, anthropic and modern risks (UoA) |

**Civil Protection Structures and Agents (University of the Azores)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| The different organizations, structures and civil protection agents are discussed regarding the structure, organization, competences and duties.  Topics of the module include:   * Public Civil Protection policies * International organizations and structures * National Civil Protection authority * Civil Protection structure * Civil Protection agents |
| **Activities & Methodology** |
| The module operates with the collaboration of leaders from different organizations, structures and entities. |
| **Evaluation / Assessment** |
| Class works 40% Practices 60% |
| **Learning outputs (Competences)** |
| **EPM A1.3** - The legal framework that determines public policies in terms of civil protection services (UoA  **EPM A2.4 -** Identify and characterize international civil protection institutions and related organizations and structures, the key actors in charge. (UoA)  **ECEM A2.2** - Identify and characterize international civil protection organizations and structures (UoA)  **EPM A2.6** - Know the key actors of the civil protection system (UoA) |

**Natural and Technological Risks (University of the Azores)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| The module aims to provide an integrated view of natural and technological risks, so the learning objectives of this module are situated, fundamentally, both around the strengthening of notions and principles, and of a better perception of public policies in the field of risk prevention, whether in their construction or implementation.  Topics of the module include:   * Hazard, vulnerability, value and risk * Multiple hazards and risks * Risk assessment (natural hazards, and environmental and technological risks) * Public policies |
| **Activities & Methodology** |
| The module operates on a seminar basis with the collaboration of experts, from the public and the private sector, on risk management. |
| **Evaluation / Assessment** |
| A written paper (60%) and its oral presentation (40%) on a topic of the module. |
| **Learning outputs (Competences)** |
| **EPM A1.4 -** The relevant legislation, public policies to mitigate natural and anthropic risks (UoA)  **ECEM A1.5** - Know public policies to reduce natural and anthropic risks in crisis management (UoA)  **EPM A3.2 -** Identify preventive measures to mitigate risk and recognize the difficulties inherent in their implementation (UoA)  **ECEM A3.2** - Identify measures to reduce/mitigate risk in crisis management and recognize the difficulties inherent in their implementation (UoA)  **ECEM A3.1** - Understand the level of complexity of risk assessment processes for the best emergency planning (UoA) |

**Crisis Management And Response Mechanisms (University of the Azores)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| Throughout history, there have been several successful and failed examples related to crisis management. This module addresses facts that contribute to complex problems to solve in the different phases of disaster management during a crisis.  Topics of the module include:   * Introduction to crisis management; * Disaster management phases; * Dissemination of information; * Case study |
| **Activities & Methodology** |
| Theoretical activities: Presentation of illustrative diagrams/photographs of the objects, concepts and processes targeted for analysis.  Practical activity: Design an exercise. |
| **Evaluation / Assessment** |
| A written paper (60%) and its oral presentation (40%) |
| **Learning outputs (Competences)** |
| **EPM D1.3** - Recognize the close link among the different phases of risk prevention management (UoA)  **ECEM D1.2** - Recognize the close link among the different phases of emergency management (UoA)  **EPM D2.2 -** Knowledge and understanding of the factors including approaches and skills that condition the success of crisis/emergency management (planning) (UoA)  **ECEM D1.3** - Understand the factors that condition the success of crisis/emergency management (UoA) |

|  |
| --- |
| Below are some modules selected from those designed and created by the **E.Di.Ma.S.** for transdisciplinary training in the European academic environment aimed at professionals of the “**Prevention Manager”** and the “**Emergency Manager**”: |

**Agenda 2030 and Emergency Management - EPM (EDIMAS)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| Environment, socioeconomics, and social security (civil defence, public health, social welfare, and civil protection) are the areas of intervention of the European Emergency Management.  This module addresses the immersive interconnections between the integrated strategic prevention of the UN 2030 Agenda and the innovative approach to the governance of the complexities related to crises and emergencies.  Module topics include:   * Introduction to the UN Agenda 2030. * Phases of integrated strategic planning. * information on European Prevention Management and Emergency Management. * Study cases. |
| **Activities & Methodology** |
| Theoretical activities: Presentation of the projects, concepts, and process cycles object of the analysis.  Practical activity: Design an exercise. |
| **Evaluation / Assessment** |
| A written paper (60%) and its oral presentation (40%) |
| **Learning outputs (Competences)** |
| **EPM A3.1** Ability to identify and apply the proper regulations to each specific Multi Risk scenario |
| **EPM D1.1** Capacity to identify the prevention plan/s referred to Major Events and related Risks |

**National and European Civil Protection - EPM (EDIMAS)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| The module provides knowledge about of “European Civil Protection system” and the characteristics that this “public service” has in the Member States.  It also provides information on the European civil protection Mechanism to which European and foreign States can request support in case of need.  Particular attention is paid to the functioning and “integration of public and private functions in local, territorial, nationale and European governance structures. |
| **Activities & Methodology** |
| Theoretical activities: Presentation of the public and private bodies that contribute to the European civil protection system, of their functioning within the Member States.  Practical activity: Design an exercise. |
| **Evaluation / Assessment** |
| A written paper (60%) and its oral presentation (40%) |
| **Learning outputs (Competences)** |
| **EPM A1.3** The legal framework that determines public policies in terms of civil protection services |
| **EPM A1.4** The relevant legislation, public policies to mitigate natural and anthropic risks. |

**National and European Civil Protection - ECEM (EDIMAS)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| The training module provides knowledge of the "European civil protection system" and of the characteristics that this "public service" has in the Member States. Particular attention is paid to:  - the activation processes of the European Civil Protection Mechanism when a European State or a foreign State makes a request for support.  - the functioning and activation of the "Operational Modules" of the European Civil Protection Mechanism |
| **Activities & Methodology** |
| Theoretical activities: Presentation of functional and process cycles within the European civil protection system  Practical activity: Design an emergency context exercise. |
| **Evaluation / Assessment** |
| A written paper (60%) and its oral presentation (40%) |
| **Learning outputs (Competences)** |
| **ECEM A1.2** Analyses and evaluate the present rules concerning the tasks and roles of each body in charge of crisis governance and emergency management |
| **ECEM A1.5** Know public policies to reduce natural and anthropic risks in crisis management |

**The Communication - ECEM (EDIMAS)**

|  |
| --- |
| **Pre-requisites** |
| None |
| **Description & Contents** |
| The module offers the ability to differentiate the tools and methods of communication strategies according to the different targets:  - recipients affected by the event / average / experts / institutions. |
| **Activities & Methodology** |
| Theoretical activities: Presentation of communication strategies and methodologies.  Practical activity: Design an exercise |
| **Evaluation / Assessment** |
| A written paper (60%) and its oral presentation (40%) |
| **Learning outputs (Competences)** |
| **ECEM D2.1** Describe the structure and roles of a multi-disciplinary team that is formed to manage crisis/emergencies |

**MIDDLESEX UNIVERSITY**

|  |  |
| --- | --- |
| **CST4220: Blockchain Anatomy and Analytics** | Sukhvinder Hara |
| EPM A3.2 | Collate evidence from various sources to maintain an audit trail |
| EPM B1.3 | Deploy appropriate tools and techniques to carry out an investigation |
| EPM B2.1 | Techniques to identify suspects |
| EPM B2.2 | Measures to facilitate seizure |
| EPM B4.2 | Blockchain artefacts in the context of a digital investigation of cryptocurrencies and crime |
| EPM B4.3 | Application of open-source investigation techniques in cryptocurrency and blockchain investigations |
| ECEM B1.1 | Cryptocurrency / blockchain visualization and analytics |
| ECEM B3.1 | Techniques to identify suspects |
| ECEM B3.3 | Measures to facilitate seizure |
| ECEM B3.4 | Appraise the developments in criminal techniques within domain |
| ECEM D3.1 | Deploy appropriate tools and techniques to carry out an investigation |
|  |  |
| **CST4230: Digital Forensics & Incident Management** | Sukhvinder Hara |
| EPM B1.3 | Procedures of examining digital evidence collection and seizure with the possible limitations in the context of constantly changing technologies |
| EPM B2.1 | Procedures and models for establishing and maintaining a physical "chain of custody” and critically evaluate their effectiveness in a variety of digital crime scenarios |
| EPM B2.2 | Appropriate tools to carry out digital forensics search and seizure independently and as part of a team |
| EPM B4.2 | Maintain a comprehensive audit trail for the production of reports and statements to be used in a court of law |
| EPM B4.3 | Investigative guidelines for digital investigations |
| ECEM A3.1 | Documentation, reporting and analysis of digital e-crimes using case scenarios |
| ECEM B1.1 | Appropriate tools to carry out digital forensics search and seizure independently and as part of a team |
| ECEM B3.1 | Forensic environment requirements |
| ECEM B3.3 | Incident response methodology |
| ECEM B3.4 | Information hiding techniques, detection and solutions |
| ECEM D3.1 | Techniques and valid procedures to carry out digital forensic investigations on current and emerging technologies |
|  |  |
| **CST4240: FinCrime Risks from Emerging Technologies** | Sukhvinder Hara |
| EPM A1.2 | Relevant regulatory frameworks for financial services, and the practice of regulatory compliance in corporate organisations |
| EPM B1.3 | Changing financial crime typologies from new emerging technologies |
| EPM B2.1 | New technologies for vulnerability to financial crime and develop prevention strategies |
| EPM B2.2 | RegTech: the use of technology to address financial crime risk |
| EPM B4.2 | Future readiness strategy development |
| EPM B4.3 | Impact assessment of new technologies in practice |
| ECEM A3.1 | Policy documents and to give advice on matters regarding compliance and crime from new emerging technologies |
| ECEM B1.1 | New technologies for vulnerability to financial crime and develop prevention strategies |
| ECEM B3.1 | Financial crime concepts and types of crime |
| ECEM B3.2 | Opportunities and vulnerabilities of adopting emerging technology for business |
| ECEM B3.4 | Understanding regulation of financial services |
| ECEM D3.1 | Assessment of new technologies |
|  |  |
| **CST4250: Open-Source Intelligence Techniques** | Sukhvinder Hara |
| EPM A1.2 | The application of investigative guidelines, ethical practices and legislation |
| EPM A1.3 | The application of investigative guidelines, ethical practices and legislation |
| EPM B1.3 | Evaluate open-source data gathering intelligence techniques and collection methodologies |
| EPM B2.1 | Various techniques for advanced searching and data gathering methods |
| EPM B2.2 | Various techniques for advanced searching and data gathering methods |
| EPM B4.2 | The application of investigative guidelines, ethical practices and legislation |
| EPM B4.3 | Advanced techniques to gather intelligence and evidence |
| ECEM A1.3 | Application of investigative guidelines, ethical practices and legislation |
| ECEM B1.1 | Open-source data gathering intelligence techniques and collection methodologies |
| ECEM B3.1 | Various techniques for advanced searching and data gathering methods |
| ECEM B3.3 | Appropriate tools (open source and specialist tools) to carry out open-source intelligence gathering |
| ECEM B3.4 | Evaluate data sources and understand their limitations |
| ECEM D3.1 | Apply advanced techniques to gather intelligence and evidence |
|  |  |
| **CST4550: Penetration Testing and Digital Forensic** | **Mahdi Aiash** |
| EPM A3.2 | Information gathering, reconnaissance and the penetration testing process |
| EPM B1.3 | Identify and solve problems, both individually and working in groups |
| EPM B2.1 | Formulate appropriate methods for troubleshooting |
| EPM B2.2 | Design and plan a penetration test in accordance with current standards and legal / ethical issues |
| EPM B4.2 | Evaluate the design of countermeasures for computer and network flaws found as a result of penetration tests |
| EPM B4.3 | Evaluate the design of countermeasures for computer and network flaws found as a result of penetration tests |
| ECEM A3.1 | Apply relevant theoretical concepts to Identify and solve problems |
| ECEM B1.1 | Attack tools, application usage and development, including writing exploits and payloads |
| ECEM B3.1 | Evaluate research and different types of information & evidence arguments critically |
| ECEM B3.3 | Apply relevant theoretical concepts to Identify and solve problems |
| ECEM B3.4 | Design and plan a penetration test in accordance with current standards |
| ECEM D3.1 | Systematically and critically evaluate the design of countermeasures for computer and network flaws found as a result of penetration tests |
|  |  |
| **CST 4560: Network Security and Services** | **Mahdi Aiash** |
| EPM A3.2 | Security threats and the available security mechanisms for combating security breaches |
| EPM B1.3 | Design and implementation of security mechanisms for a given network |
| EPM B2.1 | Security policies, services and mechanisms |
| EPM B2.2 | Hardware and software security applications |
| EPM B4.2 | Security policies, services and mechanisms |
| EPM B4.3 | Solutions for real world current and future security threats, including the implementation of innovative solutions |
| ECEM A3.1 | Security threats and the available security mechanisms for combating security breaches |
| ECEM B1.1 | Authentication and authorisation, intrusion detection and information security techniques |
| ECEM B3.1 | Technical security systems |
| ECEM B3.2 | Security mechanisms for a given network |
| ECEM B3.3 | Security policies, services and mechanisms |
| ECEM B3.4 | Solutions for real world current and future security threats, including the implementation of innovative solutions |
| ECEM D3.1 | Security policies, services and mechanisms |
|  |  |
| **CST 4590: Cyber Security and Legal Regulations** | **Mahdi Aiash** |
| EPM A3.2 | Risk Assessment Process |
| EPM B1.3 | Incident response planning |
| EPM B2.1 | Security programs, policies, procedures, standards and guidelines |
| EPM B2.2 | Prepare and test plans for contingencies and disasters |
| EPM B4.2 | Assess and manage risk in enterprise systems and networks |
| EPM B4.3 | Framework for cyber security and industrial IT |
| ECEM A3.1 | Risk Assessment Process |
| ECEM B1.1 | Disaster recovery planning |
| ECEM B3.1 | Prepare and test plans for contingencies and disasters |
| ECEM B3.2 | Design awareness, training and education programs |
| ECEM B3.3 | Identify common threats to applications, systems and networks |
| ECEM B3.4 | Assess and manage risk in enterprise systems and networks |
| ECEM D3.1 | Develop security programs, policies, procedures, standards and guidelines appropriate for corporate environments |
|  |  |
| **BIS3228: Digital Evidence** | **George Dafoulas** |
| EPM A1.1 | Law foundations in relation to forensic computing |
| EPM A4.1 | Computer related crime / Sources of legal information |
| EPM B4.1 | Investigation techniques |
| EPM B4.3 | Investigation techniques |
| EPM D4.2 | E-Crime detection / Crime interception |
| ECEM A1.6 | Law foundations in relation to forensic computing |
| ECEM A1.7 | The role of the computer forensic professional |
| ECEM A3.3 | Incidence handling |
| ECEM D2.3 | Incidence handling |
| ECEM D3.1 | Evidence presentation |
|  |  |
| **Risk Management Principles (no module code)** | **Simon McCarthy (SM), John Watt (JW), David Thomas (DT)** |
| EPM A3.3 | Risk management frameworks and governance concepts (IRGC and ISO guidance) |
| EPM B1.3 | Social impacts and vulnerability to flooding (western Europe) |
| EPM B2.1 | Introducing flood warning and emergency response |
| EPM B2.2 | Introducing flood warning and emergency response |
| EPM B3.6 | Introducing flood warning and emergency response |
| EPM D1.2 | Preventative health and safety |
| EPM D1.2 | Risk assessment challenges |
| EPM D1.2 | Tolerability of risk including frameworks and concepts such a ALARP/ALARA |
| EPM D1.2 | Built environment risk management |
| EPM D1.3 | Risk communication (perception, world views, values, biases) |
| EPM D2.2 | Business continuity |
| EPM D4.2 | Stakeholder engagement and planning |
| ECEM B2.1 | Flood defence approach, monitoring for maintenance UK |
| ECEM B2.2 | Introducing flood warning and emergency response |

A red and black logo

Description automatically generated with low confidence