FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Managing Cyberattacks Through Communication Tools
Código	E000013489
Impartido en	Master in International Security Management [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	5,0 ECTS
Carácter	Optativa
Departamento / Área	Departamento de Relaciones Internacionales
Responsable	Ileana Daniela Serban
Descriptor	Cyber-challenges and narrative information management track

Datos del profesorado

Profesor	
Nombre	Carlos Montaña Montaña
Departamento / Área	Departamento de Relaciones Internacionales
Correo electrónico	cmontana@comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Aportación al perfil profesional de la titulación

Cyber-challenges and narrative information management track

Competencias - Objetivos

Resultados de Aprendizaje

By the end of this course, students will be able to:

1. Understand key principles of crisis and internal communication.
2. Develop crisis communication strategies and tools.
3. Learn how to apply crisis communication skills specifically to managing cyberattacks.
4. Design internal communication protocols tailored to cyberattack scenarios.
5. Evaluate the effectiveness of communication during a crisis and apply lessons learned.

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Topic 1: Introduction to Crisis Communication

- **Objectives**:
  - Understand the fundamentals of crisis communication.
  - Explore the importance of effective internal communication in managing crises.
- **Content**:
  - Defining crisis communication: goals and principles.
  - The role of communication in managing organisational crises.
  - Key stakeholders and their needs during a crisis.
- **Activity**:
  - Case study analysis: How did organisations handle internal communication during a crisis (e.g., natural disasters, financial crises)?

Topic 2: Crisis Communication Models and Frameworks

- **Objectives**:
  - Explore different crisis communication models and frameworks.
  - Learn how to apply these frameworks to internal communication.
- **Content**:
  - The Situational Crisis Communication Theory (SCCT).
  - The IRT (Image Restoration Theory) and its application in internal communication.
  - Frameworks for structuring a crisis response plan.
- **Activity**:
  - Small group work: Apply SCCT to a simulated organisational crisis scenario.

Topic 3: Internal Communication Strategies in Crisis Situations

- **Objectives**:
  - Develop internal communication strategies for crisis management.
  - Understand the importance of internal trust and transparency.
- **Content**:
  - Communication strategies during the onset of a crisis.
  - Maintaining trust and transparency within the organisation.
  - Managing messaging across departments and levels.
- **Activity**:
  - Exercise: Design an internal communication plan for a company facing an unspecified crisis.

Topic 4: Internal Communication Tools for Crisis Management

- **Objectives**:
  - Learn about various internal communication tools used during crises.
  - Assess which tools work best in different crisis scenarios.
- **Content**:
  - Overview of internal communication tools.
  - Choosing the right tools based on crisis type and organisational needs.
  - How digital tools can facilitate timely and accurate internal messaging.
- **Activity**:
  - Hands-on activity: Create a mock communication campaign using specific tools in response to a mock crisis.

Topic 5: Communicating Under Pressure: Managing Stress in Crisis Communication

- **Objectives**:
  - Understand the psychological impacts of crises on communicators.
  - Learn how to manage stress and deliver clear messages under pressure.
- **Content**:
  - The role of emotions in crisis communication.
  - Techniques for managing stress while maintaining effective communication.
  - The importance of leadership and clear instructions during a crisis.
- **Activity**:
  - Role-play: Simulate a crisis and practice delivering clear internal messages under time pressure.

Topic 6: Moving from Crisis Communication to Cyber Crisis Communication

- **Objectives**:
  - Transition from general crisis communication to a focus on cyber-related crises.
  - Understand the unique challenges of internal communication during a cyberattack.
- **Content**:
  - Key differences between general and cyber-related crises.
  - Specific internal communication needs during cyberattacks.
  - Communication structures and protocols for managing a cyberattack.
- **Activity**:
  - Group discussion: Compare internal communication approaches for general vs. cyber crises.

Topic 7: The Role of IT and Security Teams in Crisis Communication

- **Objectives**:
  - Understand how IT and security teams contribute to internal communication during a cyberattack.
  - Identify key collaboration points between security and communication teams.
- **Content**:
  - Roles of IT and cybersecurity teams in managing internal communication.
  - Collaboration between communication departments and IT during a cyberattack.
  - Messaging strategies for technical vs. non-technical stakeholders.
- **Activity**:
  - Role-playing exercise: Work in teams to simulate a cyberattack and devise internal communication strategies involving IT and communication departments.

Topic 8: Crafting Internal Communication Messages During Cyberattacks

- **Objectives**:
  - Learn how to create internal messages that are clear, concise, and actionable during a cyberattack.
  - Understand the balance between transparency and confidentiality.
- **Content**:
  - Crafting messaging for different audiences: employees, management, and IT teams.
  - Key principles for clarity and urgency in crisis messaging.
  - Managing internal fears and rumors during a cyberattack.
- **Activity**:
  - Create a sample internal communication memo for employees during a simulated cyberattack.

Topic 9: Internal Communication and Cyberattack Response Time

- **Objectives**:
    - Study the critical role of response time in cyberattack management.
    - Learn strategies for managing communication in the first 24 hours of an attack.
- **Content**:
    - Importance of speed in communication during a cyberattack.
    - Designing protocols for rapid internal communication.
    - Tools to ensure rapid communication flow during an attack.
- **Activity**:
    - Develop a timeline for internal communication during a mock cyberattack, emphasising response time.

Topic 10: Internal Communication for Recovery Post-Cyberattack

- **Objectives**:
    - Understand how internal communication supports recovery after a cyberattack.
    - Develop strategies for restoring normalcy and managing internal perceptions.
- **Content**:
    - Steps for internal communication during the recovery phase.
    - Managing internal perceptions and rebuilding trust.
    - Key messaging for resuming normal operations.
- **Activity**:
    - Create a post-cyberattack internal communication plan focused on recovery.

Topic 11: Evaluating the Effectiveness of Internal Communication in Cyberattacks

- **Objectives**:
    - Learn how to assess the effectiveness of internal communication after a cyberattack.
    - Identify key performance indicators for communication during a crisis.
- **Content**:
    - Key metrics for evaluating crisis communication effectiveness.
    - Tools for feedback and post-incident analysis.
    - Lessons learned from past cyberattack communication failures and successes.
- **Activity**:
    - Develop an internal communication audit plan to evaluate a hypothetical cyberattack response.

Topic 12: Legal and Ethical Considerations in Internal Cyberattack Communication

- **Objectives**:
    - Understand the legal and ethical challenges of communicating during a cyberattack.
    - Learn about data privacy, transparency, and internal compliance during crises.
- **Content**:
    - Ethical dilemmas in internal communication during cyberattacks.
    - Balancing transparency with confidentiality in communications.
- **Activity**:
    - Group debate: Discuss real-world cases where legal and ethical issues arose in cyberattack communications.

Topic 13: Final Project: Internal Communication Strategy for a Cyberattack

- **Objectives**:
    - Apply learned concepts to design a comprehensive internal communication strategy for a cyberattack scenario.
    - Present and justify internal communication strategies based on course learnings.

- **Content**:
  - Synthesise all course concepts into a final strategy for internal communication during a cyberattack.
  - Present final projects to peers and receive feedback.
- **Activity**:
  - Final group project: Develop and present a detailed internal communication strategy for an organisation facing a simulated cyberattack.

Topic 14: Course Reflection and Feedback

- **Objectives**:
  - Reflect on the course's content and learning outcomes.
  - Discuss the future of internal communication in cyberattack scenarios.
- **Content**:
  - Recap of key lessons from the course.
  - Future trends in cyberattack communication and crisis management.
- **Activity**:
  - Final reflections: Write a short reflection on what was learned during the course and how it can be applied in the future.

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Lectures and Readings: Core concepts and frameworks will be introduced during the lectures, while preparatory readings and materials will be shared in advance.

Case Study Analysis: Students apply theoretical knowledge to real-world case studies, fostering critical thinking.

Group Discussions: In-class debates on emerging threats, international policies, and ethical concerns.

Simulation Exercises: Hands-on simulations.

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Evaluation	(%)
Final project	50%
Participation	20%
In-class exercises	30%

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

TBC for each activity.