



Unidad formativa I: Resiliencia en el Turismo

Tourism Resilience Education in Digital Security



Co-funded by
the European Union

ÍNDICE

INTRODUCCIÓN.....	3
UNIDAD FORMATIVA 1: RESILIENCIA EN EL TURISMO.....	6
Objetivos del curso.....	6
Resultados de aprendizaje.....	10
Marco y metodología de la unidad	11
2.1 Introducción a la resiliencia.....	12
1. Contenidos teóricos (6 horas)	17
2. Competencias desarrolladas en el módulo.....	18
3. Casos concretos por región (2 horas).....	19
4. Resultados esperados (6 horas).....	33
5. Evaluación (2 horas).....	40
2.2 Resiliencia y transiciones gemelas (verde y digital).....	44
2.2.1 Impacto climático y gestión de recursos (2 horas).....	45
1. Teoría que se impartirá (1 hora)	47
2. Competencias desarrolladas en la unidad	48
3. Casos prácticos (1 hora).....	48
2.2.2 Tecnologías inteligentes (SmartTech) para la resiliencia (2,5 horas).....	51
1. Contenidos teóricos (1,5 horas).....	53
2. Competencias desarrolladas en la unidad	55
3. Casos concretos (1 hora).....	56
2.2.3 El marco europeo y los destinos inteligentes (2,5 horas).....	58
1. Contenidos teóricos (1 hora).....	60
2. Competencias desarrolladas en esta unidad	60
3. Casos concretos por región (1,5 horas)	61
2.2.4 Colaboración y ecosistema (2 horas)	72
1. Teoría (1 hora)	74
2. Competencias desarrolladas en esta unidad	74
3. Casos específicos (1 hora)	75

Unidad formativa I: Resiliencia en el Turismo

2.2.5 Actividades en grupo y resultados (7 horas).....	76
2.3 Planificación de la resiliencia en el turismo.....	86
1. Marco teórico. El ciclo de vida de una crisis	89
2. Competencias adquiridas	89
3. Estudios de casos	90
4. Dinámica de trabajo y resultados esperados.....	92
5. Evaluación.....	95
REFERENCIAS	98

LISTA DE FIGURAS

Figura 1: La matriz de riesgos.....	34
-------------------------------------	----

LISTA DE TABLAS

Tabla 1: Ejemplo de un entregable.....	35
Tabla 2: Ejemplo de una matriz de sinergias.....	79

El turismo es uno de los sectores económicos más expuestos a la incertidumbre, la disrupción y el cambio rápido. Las organizaciones y los destinos turísticos operan en el seno de sistemas complejos que dependen del transporte, las infraestructuras, las comunidades locales, los recursos naturales, las plataformas digitales, las autoridades públicas, los proveedores y la confianza de los clientes. Como resultado, una interrupción en una parte de este ecosistema puede afectar rápidamente a la continuidad, la reputación y la viabilidad financiera de toda la actividad turística.

Las recientes emergencias sanitarias, los fenómenos meteorológicos extremos, la inestabilidad geopolítica, los ciberataques, los fallos en las infraestructuras y los cambios repentinos en la demanda turística han demostrado que la resiliencia ya no es una cualidad organizativa opcional. Se trata de una capacidad profesional fundamental que permite a las empresas y a los destinos turísticos anticipar riesgos, prepararse para las interrupciones, responder de forma eficaz durante una crisis, restablecer las operaciones esenciales y aprender de la experiencia.

Este curso presenta la resiliencia como un proceso dinámico y continuo, más allá de la mera capacidad de volver a la normalidad tras una crisis. Una organización turística resiliente es capaz de identificar sus vulnerabilidades, reconocer señales de alerta temprana, proteger a las personas y los activos críticos, mantener los servicios esenciales y adaptar sus procedimientos cuando cambian las condiciones. También entiende que la recuperación no debe limitarse a restablecer la situación anterior, sino a fortalecer la organización y reducir su exposición a riesgos similares en el futuro.

El curso adopta un enfoque sistémico que conecta la resiliencia organizativa con la resiliencia de la comunidad y del destino. Un hotel, un restaurante, una agencia de viajes, una atracción turística o un proveedor de transporte no puede ser completamente resiliente de forma aislada. Su capacidad para seguir operando depende de la preparación de su personal, la fiabilidad de su infraestructura digital y física, la resiliencia de los proveedores y los servicios públicos locales, y la capacidad de las partes interesadas para cooperar en situaciones de emergencia. Por este motivo, los alumnos analizarán la resiliencia a nivel individual, organizativo, comunitario y del destino.

Una característica central del curso es la integración de la resiliencia con las transiciones verde y digital. La adaptación al clima, la gestión eficiente de los recursos, las prácticas de economía circular, las tecnologías inteligentes, la inteligencia artificial, el Internet de las Cosas y los datos compartidos sobre el turismo pueden mejorar la eficiencia operativa y la preparación ante crisis. Sin embargo, estos avances también pueden generar nuevas vulnerabilidades cuando las tecnologías se implementan sin medidas adecuadas de ciberseguridad, protección de datos y planes de contingencia. Por ello, el curso anima a los estudiantes a comprender la sostenibilidad, la digitalización y la seguridad como dimensiones interconectadas de la resiliencia turística moderna.

La formación también hace especial hincapié en el factor humano. La tecnología y los procedimientos formales son importantes, pero una gestión eficaz de las crisis depende, en última instancia, de la capacidad del personal para reconocer señales de alerta, comunicarse con claridad, cooperar con los demás, tomar decisiones responsables y mantener la capacidad de adaptación bajo presión. Por ello, los alumnos desarrollarán no solo conocimientos técnicos, sino también habilidades de trabajo en equipo, liderazgo, comunicación, establecimiento de prioridades y resolución de problemas.

El curso consta de tres subunidades interrelacionadas. La primera establece las bases conceptuales y operativas de la resiliencia, incluyendo la identificación de riesgos, la evaluación de vulnerabilidades, los sistemas de alerta temprana y los factores humanos que influyen en la fiabilidad organizativa. La segunda examina cómo las soluciones ecológicas y digitales pueden reforzar la resiliencia turística mediante la adaptación al clima, la eficiencia en el uso de los recursos, las tecnologías inteligentes, los marcos europeos y la cooperación entre las partes interesadas. La tercera se centra en la planificación práctica de la resiliencia, la respuesta a las crisis, la recuperación, la gestión de la reputación y el aprendizaje tras la crisis.

El aprendizaje se apoya en casos reales de turismo, ejercicios de mapeo de riesgos, simulaciones, talleres en grupo, actividades de juego de roles y la elaboración de resultados profesionales. Estos incluyen matrices de riesgos, planes de resiliencia, informes de diagnóstico, protocolos de cooperación, materiales de comunicación en situaciones de crisis y revisiones posteriores a la acción. Las actividades están diseñadas para ayudar a los estudiantes a convertir los conocimientos teóricos en herramientas prácticas que puedan aplicarse en empresas y destinos turísticos.

Al finalizar el curso, los estudiantes deberán estar mejor preparados para contribuir activamente a la resiliencia de su organización, cooperar con las partes interesadas

Unidad formativa I: Resiliencia en el Turismo

internas y externas y apoyar unos servicios turísticos más seguros, sostenibles, protegidos digitalmente y capaces de adaptarse a los retos futuros.



Objetivos del curso

El objetivo general del curso es proporcionar a los estudiantes los conocimientos, las habilidades prácticas y las competencias profesionales necesarias para identificar, evaluar y gestionar los riesgos que afectan a las organizaciones y destinos turísticos, y contribuir eficazmente a la planificación de la resiliencia, la respuesta ante crisis, la continuidad del negocio y la recuperación tras la crisis.

El curso tiene como objetivo permitir que los estudiantes comprendan la resiliencia como una capacidad organizativa integrada que combina la gestión de riesgos, la sostenibilidad, la digitalización, la ciberseguridad, la cooperación con las partes interesadas, la comunicación en situaciones de crisis y la mejora continua.

Al finalizar el curso, los alumnos serán capaces de:

1. Comprender el concepto de resiliencia en el turismo

Explicar los principios fundamentales de la resiliencia organizativa, comunitaria y de destino, y reconocer su importancia para la continuidad, la competitividad y la sostenibilidad a largo plazo de las actividades turísticas.

2. Identificar riesgos y vulnerabilidades

Reconocer los principales riesgos sanitarios, climáticos, medioambientales, geopolíticos, operativos, humanos y digitales que pueden afectar a las empresas y a los destinos turísticos.

3. Evaluar y priorizar los riesgos

Aplicar herramientas básicas de gestión de riesgos, incluidas matrices de probabilidad e impacto, para evaluar la gravedad de las amenazas identificadas y determinar prioridades para las medidas preventivas y correctivas.

4. Reconocer señales de alerta temprana

Identifica indicadores y señales de alerta que puedan indicar la escalada de una crisis y comprende cómo una intervención temprana puede reducir el daño operativo, financiero y reputacional.

5. Comprender el ciclo de vida de la crisis

Describir y aplicar las cinco fases de la gestión de crisis —prevención, preparación, respuesta, recuperación y aprendizaje— en situaciones relacionadas con el turismo.

6. Contribuir a la resiliencia y a los planes de respuesta ante crisis

Apoyar el desarrollo de planes operativos básicos que definan medidas preventivas, funciones, responsabilidades, canales de comunicación, procedimientos de respuesta y acciones de recuperación.

7. Tomar decisiones fundamentadas bajo presión

Prioriza las acciones en situaciones de crisis, distinguiendo entre tareas urgentes y medidas vitales para proteger a las personas, las infraestructuras, los datos, las operaciones y la reputación de la organización.

8. Integrar la sostenibilidad en la planificación de la resiliencia

Comprender cómo la adaptación al cambio climático, el uso responsable de los recursos, los principios de la economía circular y los Objetivos de Desarrollo Sostenible pueden reducir la vulnerabilidad y mejorar la resiliencia a largo plazo de las organizaciones turísticas.

9. Identificar sinergias verdes y digitales

Evalúa cómo las tecnologías digitales pueden contribuir a la sostenibilidad medioambiental, la eficiencia de los recursos, la prevención de riesgos y la continuidad operativa en las empresas y los destinos turísticos.

10. Evalúa las tecnologías inteligentes aplicadas al turismo

Reconocer el posible uso de sensores del Internet de las cosas (IoT), inteligencia artificial, Big Data, sistemas de alerta temprana e infraestructuras de destinos turísticos inteligentes para supervisar riesgos, gestionar recursos y apoyar la respuesta ante crisis.

11. Reconocer las vulnerabilidades digitales

Identificar los riesgos de ciberseguridad y protección de datos asociados a los sistemas de turismo digital, los dispositivos conectados, las plataformas de reservas, las bases de datos de clientes y las infraestructuras inteligentes.

12. Aplicar principios básicos de ciberresiliencia

Comprender la importancia de la ciberhigiene, la gestión segura de datos, el aislamiento de sistemas, las copias de seguridad, la protección de redes y la ciberseguridad desde el diseño para mantener la continuidad del negocio turístico.

13. Relacionar las prácticas de resiliencia con los marcos europeos

Reconocer la relevancia de los Objetivos de Desarrollo Sostenible, el Pacto Verde Europeo, la Estrategia Digital de la UE, los modelos de Destinos Turísticos Inteligentes y otras iniciativas europeas que apoyan la transición verde y digital del turismo.

14. Cooperar con las partes interesadas pertinentes

Identificar a las autoridades públicas, los proveedores de tecnología, las asociaciones turísticas, los proveedores y las organizaciones comunitarias que deben participar en la planificación de la resiliencia y la gestión de crisis.

15. Elaborar protocolos de cooperación

Definir las responsabilidades básicas, los procedimientos de comunicación y los mecanismos de colaboración entre las empresas turísticas, las autoridades públicas y los proveedores de tecnología antes, durante y después de una crisis.

16. Comunicar los riesgos con claridad

Traducir la información técnica o compleja sobre riesgos en mensajes claros y comprensibles para directivos, empleados, clientes y otras partes interesadas sin conocimientos técnicos.

17. Participar de forma eficaz en simulacros de crisis

Desempeñar un papel activo en comités de crisis, actividades de simulación y ejercicios en grupo, demostrando capacidad de cooperación, adaptabilidad, toma de decisiones responsable y habilidades para la resolución de problemas.

18. Gestionar la comunicación de crisis y la reputación

Preparar respuestas adecuadas para los clientes, los medios de comunicación y las plataformas en línea, utilizando la empatía, la transparencia y la información precisa para ayudar a restablecer la confianza tras una crisis.

19. Apoyar la recuperación tras la crisis

Proponer medidas para restablecer los servicios esenciales, la confianza de los clientes, la estabilidad financiera, las operaciones digitales y la reputación de la organización tras una interrupción.

20. Aplicar las lecciones aprendidas tras la crisis y la mejora continua

Llevar a cabo análisis básicos posteriores a la crisis, identificar los puntos débiles de la respuesta de la organización y recomendar medidas preventivas y ajustes para reforzar la resiliencia futura.

21. Demostrar autonomía y responsabilidad profesionales

Llevar a cabo tareas rutinarias relacionadas con la resiliencia de acuerdo con los procedimientos establecidos, asumir la responsabilidad de las acciones asignadas y reconocer cuándo un problema debe remitirse a especialistas técnicos o a la alta dirección.

22. Elaborar herramientas prácticas de resiliencia

Elaborar productos profesionales tales como matrices de riesgos, mapas de riesgos, planes de resiliencia, informes de diagnóstico inteligentes, planes de sinergia, acuerdos de cooperación, matrices de priorización, materiales de comunicación de crisis e informes de análisis posterior a la acción.

Al finalizar el curso, los alumnos serán capaces de contribuir de manera significativa a la resiliencia de una empresa turística o un destino. Serán capaces de identificar riesgos, proponer medidas preventivas, apoyar la planificación ante crisis, participar en respuestas coordinadas y contribuir a estrategias de recuperación que protejan a las personas, las operaciones, los datos, los recursos y la reputación de la organización.

Resultados del aprendizaje

CONOCIMIENTOS

Al finalizar la formación, el alumno será capaz de explicar los conceptos clave de la resiliencia organizativa y comunitaria y comprender su relevancia para el sector turístico. Podrá identificar los principales factores de riesgo y vulnerabilidad que pueden afectar a las actividades turísticas, incluidos los riesgos sanitarios, climáticos, geopolíticos y digitales. El alumno también será capaz de describir la relación entre la resiliencia y las transiciones ecológicas y digitales en curso en el turismo, y de reconocer los marcos políticos europeos pertinentes, como los Objetivos de Desarrollo Sostenible (ODS), el Pacto Verde de la UE y la Estrategia Digital de la UE. Además, comprenderá los principios básicos de la gestión de crisis y la recuperación tras una crisis en las organizaciones turísticas.

COMPETENCIAS

Los alumnos serán capaces de identificar y evaluar los riesgos y vulnerabilidades de una empresa turística o un destino. Podrán contribuir al desarrollo de planes básicos de resiliencia y respuesta ante crisis, aplicando principios de sostenibilidad y digitalización para reforzar la resiliencia del turismo. Además, los alumnos participarán de forma eficaz en simulacros de crisis y actividades de juego de roles, y apoyarán las estrategias de recuperación tras un escenario de crisis en el contexto turístico.

COMPETENCIAS

Los alumnos demostrarán un grado de autonomía a la hora de realizar tareas rutinarias relacionadas con la resiliencia, siguiendo los procedimientos establecidos. Cooperarán con sus compañeros y otras partes interesadas durante situaciones de crisis y asumirán la responsabilidad de aplicar medidas de resiliencia dentro de su función en una organización turística.

Marco y metodología de la unidad

DURACIÓN

48 horas (16 por cada subunidad)

MÉTODOS DE IMPARTICIÓN

La unidad puede impartirse en línea, de forma presencial o mediante aprendizaje en grupo.

ACTIVIDADES PRÁCTICAS Y RESULTADOS RELACIONADOS

- Análisis de ejemplos reales de destinos resilientes, seguido de la redacción de un informe
- Taller en grupo: diseño de planes de resiliencia adaptados a diferentes destinos, que culminará con la redacción de un Plan Integral de Resiliencia Turística y una presentación en grupo ante el formador y el resto de alumnos
- Actividad de juego de roles: simulación del proceso de toma de decisiones de un comité de gestión hotelera durante una crisis, seguida de la redacción de un informe de análisis

Las actividades prácticas pueden realizarse de forma individual o en grupo, dependiendo del contexto.

EVALUACIÓN

- Cuestionarios en línea sobre los marcos europeos y los ODS
- Evaluación de las actividades prácticas mediante, por ejemplo, cuestionarios, pruebas, hackatones, informes y presentaciones en grupo

El rendimiento de los alumnos se evaluará en función de su capacidad para identificar y clasificar correctamente los riesgos en un caso práctico turístico concreto y para demostrar una toma de decisiones adecuada durante escenarios de crisis simulados. Contribuirán a la elaboración de planes de acción de resiliencia, escritos u orales, para organizaciones turísticas y participarán activamente en juegos de rol y actividades en grupo, demostrando habilidades para la resolución de problemas y el trabajo en equipo. Además, se espera que los alumnos completen pruebas o cuestionarios basados en conocimientos con resultados satisfactorios.

2.1 Introducción a la resiliencia

Al finalizar esta subunidad, los alumnos serán capaces de identificar vulnerabilidades en una empresa turística o un destino, evaluar la probabilidad y el impacto de los riesgos, reconocer los indicios de posibles crisis y comunicar los riesgos a partes interesadas sin conocimientos técnicos.

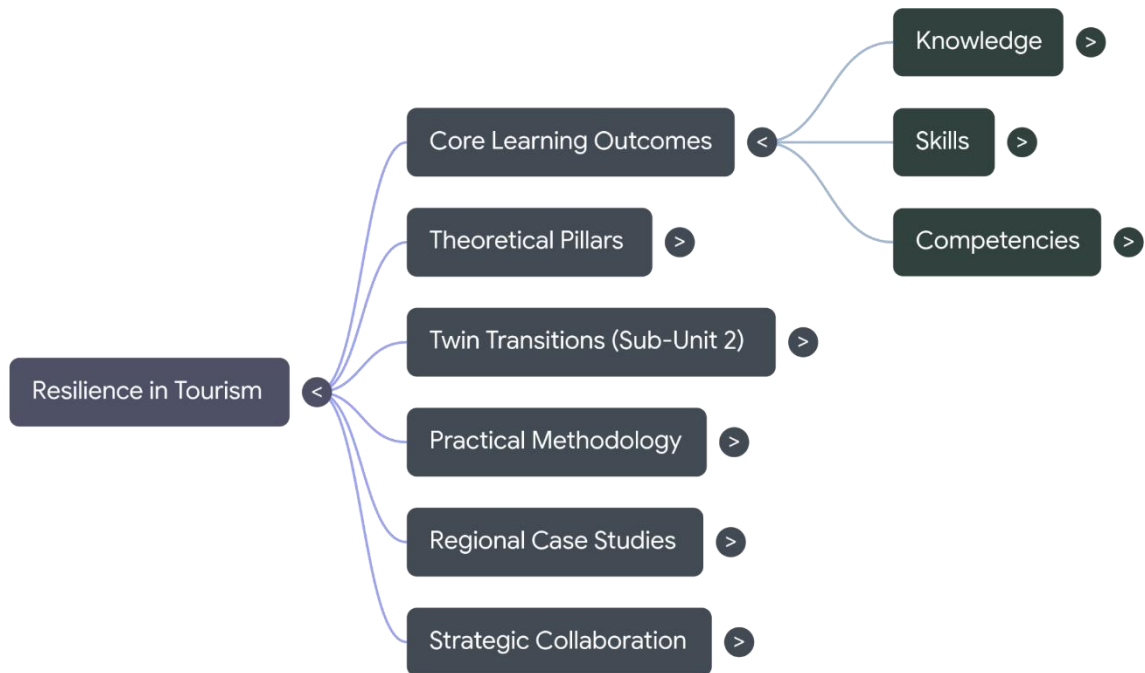
- Tipos de resiliencia (resiliencia organizativa, resiliencia comunitaria, resiliencia del destino) y su relevancia para el sector turístico
- El factor humano en la resiliencia (adaptabilidad del personal, liderazgo, trabajo en equipo, bienestar mental)
- Factores de riesgo y vulnerabilidad en el turismo (por ejemplo, desastres naturales, pandemias, inestabilidad geopolítica, amenazas digitales)
- Sistemas de alerta temprana (indicadores y señales de agravamiento de la crisis)
- Actividad práctica sugerida:
 - Ejercicio de mapeo de riesgos para un pequeño hotel o una agencia de viajes

En un mundo caracterizado por la volatilidad y el cambio constante, la capacidad de una organización para resistir, adaptarse y prosperar ante la adversidad ya no es una

opción, sino un requisito esencial para la competitividad y la confianza en la era digital.

Esta unidad parte de la premisa de que la resiliencia en el turismo no es un estado estático, sino un proceso dinámico que abarca desde el nivel individual y organizativo hasta la comunidad y el destino en su conjunto. Los alumnos aprenderán que ser resiliente implica una comprensión profunda de los factores de riesgo y vulnerabilidad que pueden afectar al sector, incluyendo no solo los desastres naturales o las crisis sanitarias, sino también los riesgos geopolíticos y, lo que es más importante, las amenazas digitales emergentes.

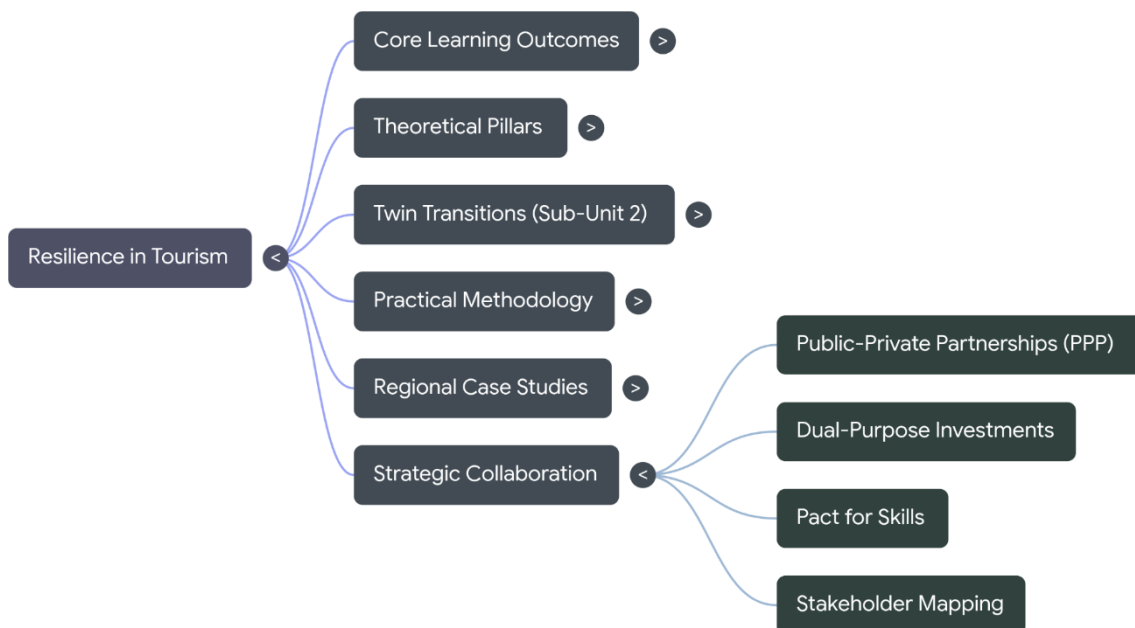
Esquema de la unidad



Unidad formativa I: Resiliencia en el Turismo



Unidad formativa I: Resiliencia en el Turismo



1. Contenidos teóricos (6 horas)

Este módulo sienta las bases conceptuales para entender la resiliencia como una capacidad operativa y no como una capacidad estática.

El marco teórico en el que se basa la formación se inspira en la **Teoría de los Sistemas Socioecológicos (SES)** y en la **Teoría de las Organizaciones de Alta Fiabilidad (HRO)**, adaptadas específicamente al contexto del programa TREADS.

Para sustentar esta unidad, el contenido debe estructurarse en torno a cuatro pilares teóricos principales que permitan al alumno comprender la resiliencia no como un concepto estático, sino como una capacidad operativa.

I. Teoría de los sistemas socioecológicos (SES)

Esta teoría explica la interdependencia entre el sector turístico, la comunidad y el medio ambiente.

Resiliencia del destino: El curso parte de la premisa de que un hotel o una agencia no es una isla; su supervivencia depende de la infraestructura y la seguridad de todo el destino.

Interconectividad: analiza cómo los riesgos en un área (por ejemplo, un ciberataque a los sistemas de suministro) afectan a la resiliencia de la comunidad local y a la reputación del sector.

II. El ciclo de vida de la crisis (teoría de la gestión de crisis)

Este es el modelo de referencia para comprender las fases de una perturbación.

Prevención y preparación: Conocimientos sobre la identificación proactiva de señales de alerta temprana (EWS) para mitigar los riesgos antes de que se agraven.

Respuesta y recuperación: Teoría sobre la movilización de recursos y la toma de decisiones bajo presión para restablecer la normalidad operativa.

Aprendizaje tras la crisis: el concepto de «crecimiento postraumático» organizativo, en el que la empresa aprovecha la crisis para reforzar sus puntos débiles.

III. Teoría de las organizaciones altamente fiables (HRO)

Este marco es esencial para documentar el **factor humano**. Se centra en organizaciones que operan en entornos de alto riesgo (como el turismo digitalizado) sin cometer errores catastróficos.

Concienciación sobre los fallos: Fomentar la mentalidad de que cualquier anomalía menor (un correo electrónico sospechoso, un retraso técnico) podría ser el inicio de una crisis.

Sensibilidad operativa: el reconocimiento de que el personal de primera línea es el más indicado para detectar las vulnerabilidades del día a día.

Respeto por la experiencia: en una crisis, la toma de decisiones debe recaer en quienes poseen conocimientos técnicos (por ejemplo, el experto en seguridad digital), y no necesariamente en quienes ocupan el rango jerárquico más alto.

IV. Modelo de gestión de riesgos (matriz de probabilidad e

Esta es la base técnica del ejercicio de **mapeo de riesgos**.

Cuantificación del riesgo: Los alumnos deben aprender a asignar valores numéricos o cualitativos a la probabilidad de que se produzcan amenazas climáticas, geopolíticas o digitales, así como a su impacto potencial.

Priorización estratégica: Teoría sobre cómo decidir qué riesgos ignorar, cuáles mitigar y cuáles transferir (por ejemplo, mediante seguros o redundancia de sistemas).

2. Competencias desarrolladas en el módulo

- **Identificación y evaluación de riesgos:** capacidad para detectar vulnerabilidades específicas en una empresa o un destino turístico, asignando valores de probabilidad e impacto para priorizar las amenazas climáticas, geopolíticas o digitales.
- **Gestión proactiva y alerta temprana:** Capacidad para reconocer señales y «señales de alarma» (sistemas de alerta temprana —EWS—) que indican la escalada de una crisis, lo que permite tomar medidas antes de que la situación se salga de control.
- **Comunicación estratégica con partes interesadas sin conocimientos técnicos:** Capacidad para «traducir» amenazas técnicas complejas (como los ciberataques) en información comprensible para directivos, empleados y clientes, facilitando así la toma de decisiones informadas.

- **Toma de decisiones y autonomía bajo presión:** la capacidad de priorizar las acciones críticas durante una crisis, asumir la responsabilidad de las tareas rutinarias de resiliencia y dar prioridad a la protección de datos frente a las operaciones inmediatas si es necesario.
- **Cooperación y gestión del factor humano:** Capacidad para colaborar con compañeros y partes interesadas externas durante situaciones de emergencia, fomentando la adaptabilidad y el liderazgo dentro del equipo.
- **Aplicación de medidas de ciberhigiene:** Capacidad para aplicar protocolos técnicos básicos, como la formación en detección de *phishing*, el aislamiento de sistemas comprometidos y el cumplimiento de normativas como el RGPD y la Directiva NIS2.

3. Casos específicos por región (2 horas)

Para facilitar el aprendizaje, se utiliza el **Hotel Horizonte** (50 habitaciones, ubicación costera, riesgo de inundaciones y alta dependencia digital) como escenario cambiante para todas las actividades.

1. España: Análisis de la erupción en La Palma («Resiliencia del destino»), la tormenta Filomena («Factor humano»), la quiebra de Thomas Cook («Dependencia del canal») y el ciberataque a Lopesan («Higiene cibernética»)

A. Resiliencia del destino: La erupción del volcán Cumbre Vieja (La Palma, 2021)

- **Contexto:** La erupción destruyó infraestructuras clave y paralizó el turismo en el valle de Aridane.
- **Teoría aplicada:** Sistemas socioecológicos (SES). El hotel no es una isla; su supervivencia dependía de la red de seguridad del destino y de la gestión del Cabildo.
- **Lección para el alumno:** Identificación de las vulnerabilidades geográficas y la importancia de los sistemas de alerta temprana volcánica (EWS).
- **Acción resiliente:** El uso de vales turísticos y un giro hacia el «turismo vulcanológico» para transformar el desastre en una oportunidad de aprendizaje tras la crisis.



Enormes rocas flotan por los ríos de lava de la erupción del volcán de La Palma

B. Vulnerabilidad económica: La quiebra de Thomas Cook (Islas Canarias e Islas Baleares, 2019)

- **Contexto:** La quiebra del operador turístico más antiguo del mundo dejó a 70 000 turistas británicos varados en España y a los hoteles con una deuda de millones.
- **Teoría aplicada:** Matriz de riesgos (priorización estratégica).
- **Lección para el alumno:** El riesgo de depender de un único canal. Evaluar el impacto de una amenaza geopolítica o económica externa en el flujo de caja de la empresa.
- **Medida de resiliencia:** Diversificación de los mercados emisores y aceleración de la digitalización para vender directamente al cliente (B2C), reduciendo así el poder de los grandes operadores turísticos.



La quiebra de Thomas Cook causó conmoción en todo el sector

C. Crisis ecológica y de reputación: el Mar Menor (Murcia)

- **Contexto:** La crisis de anoxia y eutrofización en la laguna salina ha provocado un descenso sistemático de la demanda y del valor de los inmuebles.
- **Teoría aplicada:** Teoría de las organizaciones de alta fiabilidad (HRO).
- **Lección para el estudiante:** Sensibilidad operativa. Detectar las «señales de alerta temprana» medioambientales (clorofila, turbidez) antes de que la crisis afecte a la reputación general del destino.
- **Acción resiliente:** Puesta en marcha del proyecto BELICH (2026) para anticipar crisis ecológicas mediante modelos de predicción inteligentes.



La laguna española del Mar Menor obtiene la personalidad jurídica, una primicia en Europa • FRANCE 24 English

2. Italia: el sistema MOSE en Venecia (infraestructuras), las inundaciones en las Cinque Terre (conservación del paisaje) y la digitalización de las pymes tras la pandemia

A. Resiliencia del destino: Venecia y el sistema MOSE + Precio de la entrada

- **Contexto:** La ciudad se enfrenta a la doble amenaza del aumento del nivel del mar (*Acqua Alta*) y del «turismo excesivo», que está ahuyentando a los residentes.
- **Teoría aplicada: Resiliencia del destino e infraestructuras críticas.** El MOSE es una barrera física contra las inundaciones, mientras que la tarifa de entrada es una herramienta para gestionar los flujos de visitantes.
- **Lección para el estudiante:** Cómo un destino debe proteger tanto su patrimonio físico (frente al clima) como su tejido social (frente a la masificación) para seguir siendo viable.
- **Medida de resiliencia:** Uso de tecnología hidráulica a gran escala y de sistemas digitales de reserva y pago para regular la capacidad de acogida del destino.



[Venecia se está hundiendo: un experto en ingeniería explica cómo salvarla | WSJ Pro Perfected](#)

B. Recuperación tras el desastre: Cinque Terre y las inundaciones de 2011 (Vernazza)

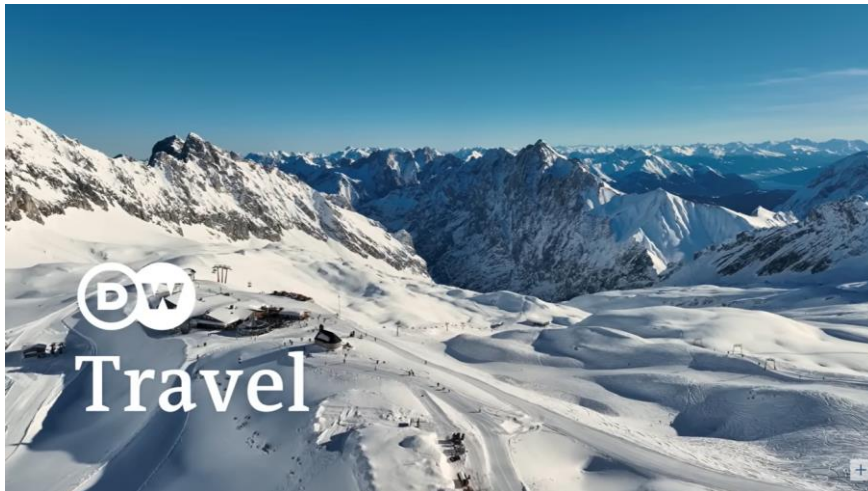
- **Contexto:** En octubre de 2011, unas lluvias torrenciales provocaron inundaciones y deslizamientos de tierra catastróficos que sepultaron el pueblo de Vernazza bajo metros de barro.
- **Teoría aplicada:** Ciclo de vida de una crisis (respuesta y recuperación). La fragilidad del paisaje aterrazado de Cinque Terre es un punto crítico de fallo.
- **Lección para el alumno:** La importancia de la conservación del paisaje como infraestructura. El abandono de las terrazas agrícolas aumentó la inestabilidad del suelo.
- **Acción resiliente:** Reconstrucción basada en la restauración de los muros tradicionales de piedra seca y la creación de un plan integrado de gestión del agua para prevenir futuros desprendimientos.



Inundación en Vernazza, 25/10/2011, 18:17

C. Riesgo climático y estacionalidad: las Dolomitas y la nieve artificial

- **Contexto:** El aumento de las temperaturas está acortando la temporada natural de esquí en los Alpes italianos, lo que afecta a la economía invernal de regiones como Trentino-Alto Adige.
- **Teoría aplicada: Sistemas socioecológicos (SES) y gestión de recursos.** La dependencia del agua para producir nieve entra en conflicto con las necesidades de la comunidad durante las sequías.
- **Lección para el estudiante:** Identificar la vulnerabilidad de la estacionalidad. Cómo diversificar el modelo de negocio hacia el «turismo de cuatro estaciones» para evitar depender exclusivamente de las condiciones meteorológicas.
- **Acción resiliente:** Diversificación hacia el senderismo guiado digitalmente, el cicloturismo y el uso de embalses de almacenamiento de agua polivalentes.



Deportes de invierno: cómo está afectando el cambio climático a las estaciones de esquí

3. Eslovenia: gestión de las inundaciones récord de 2023, adaptación al cambio climático en Kranjska Gora y el programa «Destino Verde»

A. Resiliencia climática: adaptación en Kranjska Gora y Planica

- **Contexto:** Las estaciones de esquí de baja altitud se enfrentan a inviernos sin nieve y a una temporada de esquí más corta debido al calentamiento global.
- **Teoría aplicada:** Resiliencia ante la emergencia climática y los sistemas socioecológicos (SES).
- **Lección para el estudiante:** La vulnerabilidad del turismo estacional. Kranjska Gora está rediseñando su modelo para adoptar el «turismo de cuatro estaciones», de forma similar al caso de los Alpes franceses mencionado en el plan original.
- **Acción resiliente:** Inversión en movilidad verde digitalizada (reservas de aparcamiento y autobuses lanzadera) para gestionar los flujos turísticos a lo largo del año y proteger el medio ambiente del Parque Nacional de Triglav.



Resiliencia climática

B. Seguimiento medioambiental: Seguimiento de la cueva de Postojna

- **Contexto:** Un ecosistema kárstico extremadamente frágil que lleva más de 200 años recibiendo visitantes y que alberga especies endémicas como el proteo (los «dragones bebés»).
- **Teoría aplicada:** Teoría de las organizaciones de alta fiabilidad (HRO) y sensibilidad operativa.
- **Lección para el estudiante:** Uso de indicadores biológicos y microclimáticos como señales de alerta temprana. Cualquier cambio en la temperatura o en la calidad del aire detectado mediante sus estudios sistemáticos se utiliza para ajustar los flujos turísticos.
- **Acción resiliente:** El proyecto «Predjama Sustainable» para reducir el tráfico rodado y la contaminación de las aguas subterráneas, con lo que se ha conseguido la certificación como destino «Cero Residuos».



PARQUE DE LAS CUEVAS DE POSTOJNA - I FEEL SLOVENIA

C. Marco nacional de resiliencia: Plan Verde Esloveno para el Turismo (GSST)

- **Contexto:** Eslovenia fue el primer país del mundo en ser declarado «Destino Verde». Su programa nacional (GSST) agrupa a destinos y proveedores bajo normas de sostenibilidad.
- **Teoría aplicada:** Resiliencia del destino y de la comunidad.
- **Lección para el estudiante:** La interdependencia entre las empresas y la comunidad. El GSST ofrece herramientas de medición estandarizadas para ayudar a los hoteles a reducir los costes operativos (energía y agua) y aumentar su eficiencia.
- **Acción resiliente:** Integrar la sostenibilidad en la estrategia nacional de recuperación, condicionando las ayudas públicas a criterios de resiliencia medioambiental y social.



[Eslovenia Verde](#)  [La historia de la Eslovenia verde](#)

4. **Grecia: Evacuación por los incendios en Rodas (comunicación de crisis), gestión del exceso de turismo en Santorini y resiliencia sísmica en los hoteles**

A. Gestión de crisis en tiempo real: Incendios en Rodas (2023)

- **Contexto:** La evacuación de más de 19 000 personas debido a incendios forestales fuera de control, lo que supuso la mayor operación de evacuación de la historia del país.
- **Teoría aplicada:** Sistemas de alerta temprana (EWS) e indicadores de escalada de crisis.
- **Lección para los estudiantes:** Ilustra la importancia de la comunicación de crisis y la coordinación entre el sector privado (TUI, hoteles locales) y las autoridades públicas para dar prioridad a la seguridad de las personas por encima de todo.
- **Acción resiliente:** El uso de las redes sociales y los canales digitales para ofrecer información actualizada minuto a minuto, lo que evitó el pánico y permitió gestionar la reputación del destino incluso durante la emergencia.



Miles de personas huyen de sus hogares y hoteles en Rodas a medida que se propagan los incendios

B. Resiliencia del destino: Santorini y la gestión del «turismo excesivo»

- **Contexto:** La saturación de pasajeros de cruceros en una isla con infraestructuras limitadas pone en peligro la experiencia turística y la calidad de vida de la comunidad.
- **Teoría aplicada:** Teoría de los sistemas socioecológicos (SES). La empresa (hotel/agencia) no puede ser resiliente si el ecosistema del destino colapsa debido a la masificación.
- **Lección para el estudiante:** Identificación de los puntos críticos de fallo en la infraestructura (puertos, transporte local) y cómo el exceso de demanda puede convertirse en un riesgo operativo.
- **Acción resiliente:** Implantación de un sistema digital de gestión del flujo de cruceros (cuotas diarias) para equilibrar la economía turística con la sostenibilidad del destino.



Turismo en Santorini: Instagram frente a la realidad - En misión | ITV News

C. Factor humano y seguridad física: resiliencia sísmica en el sector hotelero

- **Contexto:** Grecia es una de las zonas con mayor actividad sísmica de Europa.
- **Teoría aplicada:** la teoría de las organizaciones de alta fiabilidad (HRO) y el factor humano.
- **Lección para los alumnos:** la capacidad de adaptación y el liderazgo del personal bajo presión. Un equipo formado en protocolos sísmicos detecta anomalías y actúa de forma autónoma, sin esperar órdenes de sus superiores, durante los primeros segundos críticos.
- **Acción resiliente:** Simulacros sistemáticos y certificaciones de seguridad estructural comunicadas de forma transparente para fomentar la confianza de los clientes (reputación).
- **Riesgo climático y salud:** el cierre de la Acrópolis debido a las olas de calor
- **Contexto:** En verano, las temperaturas extremas superan los 40 °C, lo que obliga a cerrar el monumento más visitado de Grecia para evitar golpes de calor.

5. Europa: Gestión de la confianza tras los atentados de Bruselas, fallos en la alerta temprana de la COVID-19 en Ischgl y protocolos del Eurotúnel

A. Riesgos geopolíticos y de seguridad: Bruselas (Bélgica) tras 2016

- **Contexto:** Los atentados de 2016 paralizaron el «corazón de Europa», afectando al aeropuerto y al metro, lo que provocó que la ocupación hotelera se desplomara durante meses.
- **Teoría aplicada:** Resiliencia del destino y de la comunidad. La recuperación no solo dependió de la seguridad, sino también de la confianza colectiva en los espacios públicos.
- **Lección para el estudiante:** Cómo gestionar la comunicación de riesgos en un entorno de inestabilidad geopolítica para restaurar la reputación del destino.
- **Acción resiliente:** La campaña «Call Brussels», en la que los ciudadanos respondían a las llamadas de turistas de todo el mundo para demostrar que la ciudad era segura, reforzando así el factor humano.



BÉLGICA: REFUERZO DE LA SEGURIDAD EN BRUSELAS

B. Fracaso en la alerta temprana: Ischgl (Austria) y la COVID-19

- **Contexto:** Al inicio de la pandemia en 2020, esta estación de esquí se convirtió en un foco de transmisión masiva en toda Europa porque no actuó a tiempo ante las señales de alerta.
- **Teoría aplicada:** Teoría de las organizaciones de alta fiabilidad (HRO). Se produjo un fallo en la «preocupación por los fallos» y en la detección temprana de anomalías.
- **Lección para el estudiante:** La importancia de reconocer las señales de alerta tempranas y no ignorar los indicadores en aras de intereses económicos inmediatos.
- **Acción resiliente:** Una revisión completa de sus protocolos sanitarios y de comunicación, integrando sistemas de seguimiento digital y un intercambio transparente de información para restablecer la confianza del mercado.

C. Riesgo de desastres naturales y continuidad: Grindavík (Islandia, 2023-2024)

- **Contexto:** La evacuación total de una localidad turística y el cierre intermitente de la Laguna Azul debido a erupciones volcánicas recurrentes.
- **Teoría aplicada:** Matriz de probabilidad e impacto. En este caso, el impacto es crítico y la probabilidad es muy alta.
- **Lección para el estudiante:** Realizar un mapeo dinámico de riesgos. El estudiante aprende a dar prioridad a la seguridad de las personas frente a las operaciones comerciales cuando una «señal de alerta» es inminente.
- **Acción resiliente:** Diseño de barreras físicas inteligentes y planes de evacuación digitalizados que permitan reabrir las instalaciones a las pocas horas de que cese la actividad sísmica.



La

clase

magistral de Islandia sobre gestión del riesgo volcánico en Grindavík

D. Resiliencia digital e infraestructuras: Eurotúnel (Francia-Reino Unido)

- **Contexto:** Fallos técnicos masivos o huelgas que bloquean la principal arteria de transporte entre el continente y las islas, dejando a miles de turistas varados.
- **Teoría aplicada:** Ciclo de vida de la crisis (respuesta).
- **Lección para el alumno:** Toma de decisiones bajo presión. El alumno debe simular cómo priorizar el suministro de información y servicios básicos a los clientes varados en un «punto único de fallo».
- **Acción resiliente:** Implementación de protocolos de comunicación multilingües automatizados y sistemas de redundancia técnica para garantizar que una anomalía digital no se convierta en una crisis operativa en toda regla.

4. Entregables (6 horas)

Para ayudar al alumno a pasar de la teoría a la competencia en el mundo real, estos tres resultados sirven como portfolio profesional del «**Experto en turismo resiliente y con competencias digitales mejoradas**». No se trata simplemente de tareas, sino de documentos técnicos que el alumno podrá aplicar en su empresa al día siguiente de completar el curso.

1. Matriz de riesgos personalizada

Este trabajo se centra en la capacidad de identificar y evaluar los riesgos y vulnerabilidades dentro de una empresa o un destino. El estudiante debe cuantificar las amenazas para priorizar la inversión en seguridad mediante:

- a) **Inventario de amenazas:** una lista clasificada por tipo: riesgos digitales (ciberataques), riesgos relacionados con el clima, riesgos relacionados con la salud y riesgos geopolíticos.

Escala de valoración (1-5) para las categorías anteriores:

- **Probabilidad:** desde «Muy improbable» hasta «Casi seguro».
- **Impacto:** de «Insignificante» a «Catastrófico» (pérdida total de datos o cierre de la empresa).
- **Cálculo del nivel de riesgo ($R = P * I$):** aplicación de la fórmula para clasificar los riesgos en un mapa de calor (verde, amarillo, rojo).

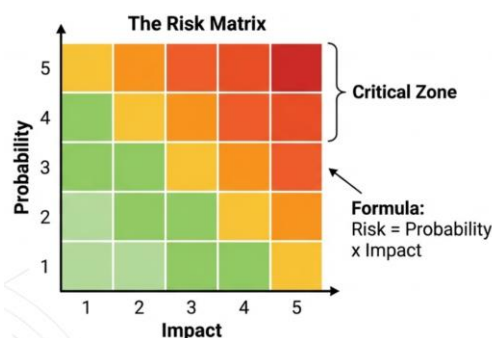


Figura1 : La matriz de riesgos

b) **Identificación y clasificación**

Amenaza: Descripción específica del suceso (p. ej., «Ransomware en el sistema de reservas» o «Inundación debida a una tormenta extrema»).

Categoría: Clasificación según los ejes del plan: **digital, medioambiental (climático), geopolítico, sanitario o humano.**

El alumno debe asignar valores del 1 al 5 para calcular la magnitud del riesgo:

- Probabilidad (P):** ¿Qué probabilidad hay de que ocurra? (1: Muy raro, 5: Frecuente).
- Impacto (I):** ¿Qué daños causaría a la continuidad del negocio? (1: Mínimos, 5: Cierre o pérdida total de datos).
- Nivel de riesgo:** El resultado de multiplicar ambos valores define la **prioridad** (baja, media, alta o crítica).

Resiliencia y estrategia de respuesta

- d. **Medida preventiva (resiliencia):** Acciones para fortalecer la organización antes de que se produzca el incidente (p. ej., formación en «ciberhigiene», protocolos de la Directiva NIS2 o seguro contra el cambio climático).
- e. **Plan de respuesta (contingencia):** Medidas que deben adoptarse *durante* la crisis para garantizar la supervivencia (p. ej., aislamiento de servidores, comunicación con las autoridades de protección de datos o evacuación).

Amenaza	Categoría	Riesgo (P × I)	Prioridad	Medida de resiliencia	Plan de respuesta
Ataque de ransomware	Digital	4 * 5 = 20	Crítico	Copias de seguridad fuera de línea y formación sobre NIS2	Aislamiento de sistemas / Protocolo de crisis
Ingeniería social	Humano	5 * 3 = 15	Inscripción	Formación en detección de fraudes	Bloqueo de cuentas / Informe de la DPA
Corte de suministro eléctrico	Operación	3 × 3 = 9	Media	Sistemas de alimentación ininterrumpida	Cambio a funcionamiento manual

Tabla1 : Ejemplo de un documento de entrega

2. Informe de análisis

Este es el documento en el que el alumno analiza críticamente su actuación tras una simulación de crisis. Este ejercicio es esencial para evaluar la capacidad del alumno para «comunicar riesgos a partes interesadas sin conocimientos técnicos» y «priorizar acciones bajo presión», tal y como se establece en el plan de formación.

Análisis crítico redactado tras la actividad *de juego de roles* («El invitado inesperado»), en el que se evalúa la toma de decisiones bajo presión y la comunicación con personal no técnico.

Este informe se redacta inmediatamente después de la actividad de simulación. Su objetivo es evaluar **las habilidades de comunicación y toma de decisiones bajo presión**.

a) Contenido del informe:

- **Cronología del incidente:** resumen de lo ocurrido durante la simulación de crisis.
- **Análisis de la comunicación:** evaluación de cómo se transmitió la información sobre riesgos a *las partes interesadas* sin conocimientos técnicos (dirección, clientes, empleados).
- **Evaluación de la cooperación:** Análisis de cómo colaboraron los compañeros y las partes interesadas durante la situación crítica.
- **Lecciones aprendidas:** Identificación de errores en la respuesta y propuestas de mejora para el futuro.

Escenario propuesto y un ejemplo detallado de cómo sería este informe.

Escenario de juego de roles: «El huésped inesperado».

Contexto: Un hotel boutique recibe un correo electrónico supuestamente procedente de una conocida agencia de viajes, en el que se solicita la confirmación urgente de una reserva de grupo para esa misma noche. El correo electrónico contiene un enlace a un «recibo de pago» que, al hacer clic en él, bloquea el acceso al sistema de gestión hotelera (PMS).

Papel:

Estudiante (recepcionista/jefe de turno): Debe detectar la anomalía, decidir si apagar el equipo e informar de la situación a la dirección y a los huéspedes que se están *registrando*.

Facilitador (director general): Un rol no técnico que da prioridad a no causar molestias a los clientes y a evitar costes adicionales.

Facilitador (técnico informático externo): Proporciona información técnica compleja que el estudiante debe «traducir».

Ejemplo de informe de análisis (rellenado por el estudiante)

- **ID de la actividad:** RP-01-Resiliencia digital
- **Estudiante:** [Nombre del estudiante]
- **Fecha:** XX/XX/202X
- **Escenario simulado:** Ataque de ransomware mediante phishing en el PMS.

Resumen del incidente (cronología)

- **10:00 h:** Recepción de un correo electrónico sospechoso que contiene un enlace externo. Se detecta una ralentización del sistema tras abrir el enlace.
- **10:15 h:** El sistema PMS muestra un mensaje de error de cifrado de archivos. Se identifica como un posible ataque *de ransomware*.
- **10:20 h:** Se decide desconectar el servidor principal de la red local para evitar la propagación (medida de contención).
- **10:30 h:** Se informa del incidente a la alta dirección y al equipo de soporte técnico.

Análisis de las acciones y la toma de decisiones

- **Aciertos:** Se aplicó el principio de «confianza cero» al sospechar del correo electrónico, aunque abrir el enlace fue el error inicial. La desconexión física del equipo impidió que el virus afectara a la base de datos de contabilidad, que se encontraba en una red independiente.
- **Retos:** Hubo un retraso inicial de 5 minutos debido a la falta de un protocolo escrito que especificara qué cables había que desconectar físicamente.

Evaluación de la comunicación (competencia clave)

- **Comunicación con las partes interesadas no técnicas:** Conseguimos explicar al director que el sistema no estaba «caído», sino «sometido a un ataque», y que la prioridad era proteger los datos de las tarjetas de crédito de los clientes por encima de la rapidez *del proceso de facturación*.
- **Gestión de clientes:** Se preparó un mensaje verbal para los clientes que esperaban en la cola, en el que se explicaba que «debido a problemas técnicos con la red» se llevaría a cabo un proceso de facturación manual temporal, manteniendo en todo momento una actitud tranquila y profesional.

Lecciones aprendidas y mejora de la resiliencia

- **Higiene cibernética:** Es necesario implementar un sistema de filtrado de correo electrónico más estricto e impartir formación específica sobre la detección *de phishing* a todo el personal de recepción.

- **Continuidad del negocio:** Debemos tener siempre a mano un «kit de emergencia» físico (formularios de registro en papel, listas de contactos de emergencia impresas) para no depender al 100 % de la red durante las primeras horas de una crisis.
- **Protocolo de notificación:** La comunicación debe ser más rápida; se perdió tiempo buscando el número de teléfono del técnico de guardia.

Marco de evaluación para el formador

Al revisar este informe, el formador debe comprobar si el alumno ha cumplido los objetivos del programa TREADS:

- ¿Ha identificado correctamente la vulnerabilidad?
- ¿Ha demostrado autonomía en las tareas rutinarias de resiliencia?
- ¿Ha dado prioridad a la protección de datos frente a las necesidades operativas inmediatas?

3. Mapa de riesgos definitivo (esquema del plan de resiliencia)

Este es el resultado más ambicioso, que actúa como hoja de ruta operativa e incluye puntos críticos, indicadores del sistema de alerta temprana (EWS), estrategias de actuación y planes de recuperación de la confianza.

- **Identificación de puntos críticos:** descripción de las vulnerabilidades específicas de su empresa (por ejemplo, dependencia de un único canal de reservas, falta de copias de seguridad externas).
- **Señales de Alerta Temprana (SAT):** definición de los indicios que anuncian una crisis (por ejemplo, ralentización inusual de la red, avisos meteorológicos oficiales, quejas sistemáticas en las redes sociales).
- **Medidas inmediatas de resiliencia:** Lista de acciones preventivas (higiene de ciberseguridad) y reactivas para garantizar la continuidad del negocio.
- **Hoja de ruta de recuperación:** estrategias básicas para restablecer la reputación y la confianza tras el incidente.

Este documento técnico se estructura en **cinco secciones clave** que transforman el análisis teórico en una hoja de ruta operativa.

1. Perfil empresarial y auditoría de vulnerabilidades

1. El alumno debe empezar por definir el ecosistema de su organización para identificar puntos débiles concretos.
 2. **Activos críticos:** Lista de elementos esenciales para el funcionamiento (por ejemplo, software de reservas, base de datos de clientes, suministro eléctrico, reputación en línea).
 3. **Puntos únicos de fallo:** identificación de los procesos que, en caso de fallo, paralizan toda la actividad (por ejemplo, la dependencia total de una única OTA o de un único servidor físico).
2. Visualización del riesgo (mapeo estratégico). Utilizando la metodología de evaluación, el alumno representa gráficamente las amenazas identificadas en una matriz técnica.
1. **Cálculo del índice de riesgo (R):** Se aplica la fórmula matemática de criticidad a cada amenaza:
 - $R = P * I$
 2. Donde P es la probabilidad de que se produzca y I es el impacto organizativo.
 - **Representación gráfica:** representación de las amenazas en un mapa de calor para visualizar las prioridades de inversión en resiliencia.
 3. Sistemas de alerta temprana (EWS). El alumno debe definir indicadores específicos que actúen como «señales de alarma» para anticipar una crisis.
 - **Indicadores digitales:** por ejemplo, un aumento inusual de los intentos fallidos de inicio de sesión o alertas de seguridad de los proveedores de tecnología.
 - **Indicadores medioambientales/sociales:** p. ej., cambios en las alertas meteorológicas oficiales o picos en las valoraciones negativas en sitios web de reseñas.
 4. Estrategia de actuación y el factor humano. Se definen medidas preventivas y reactivas, incorporando la capacidad de adaptación del personal.

- **Medidas preventivas (ecológicas y digitales):** acciones para reducir la vulnerabilidad, como la migración a la nube o protocolos de ahorro de agua en caso de sequía.
 - **Protocolo de respuesta:** asignación de funciones y responsabilidades. ¿Quién dirige la comunicación? ¿Quién se pone en contacto con el soporte técnico?
5. Estrategia de recuperación y aprendizaje. La hoja de ruta debe incluir cómo volver a la normalidad y salir fortalecidos tras el incidente.
- **Plan de continuidad:** medidas mínimas para seguir operando «en modo degradado» (p. ej., registro manual de clientes).
 - **Restablecimiento de la confianza:** estrategias de comunicación para informar a los clientes y restablecer la reputación de la marca.
 - **Revisión posterior al incidente:** protocolo para analizar qué falló y actualizar continuamente el mapa de riesgos.

Este trabajo demuestra si el estudiante ha alcanzado la autonomía necesaria para llevar a cabo tareas rutinarias de resiliencia y cooperar con otras partes interesadas en situaciones de crisis.

5. Evaluación (2 horas)

El rendimiento de los estudiantes se evaluará en función de su capacidad para:

- **Clasificar correctamente** los riesgos en un caso práctico real.
- **Demostrar autonomía** a la hora de proponer medidas de resiliencia.
- **Colaborar activamente** en el trabajo en grupo y en las presentaciones orales.

Y también a través de , un **cuestionario de evaluación:** un test de 10 preguntas sobre los fundamentos teóricos y los casos prácticos tratados en el módulo.

Preguntas:

1. ¿Cómo se define la «resiliencia del destino» según los pilares de la unidad?

- A. La capacidad de un hotel concreto para recuperar sus datos tras un ciberataque.

- B. La interdependencia entre las empresas, la comunidad y las infraestructuras para mantener la seguridad colectiva.
- C. El uso exclusivo de energías renovables en una zona turística.
- D. La capacidad de los turistas para adaptarse a cambios repentinos en las condiciones meteorológicas.

Respuesta correcta: B

2. Dentro del «factor humano», ¿cuál es un elemento crítico para la resiliencia organizativa?

- A. Instalar el software antivirus más caro del mercado.
- B. La centralización absoluta de toda la toma de decisiones en el director general.
- C. La adaptabilidad del personal, el liderazgo y el bienestar mental del equipo.
- D. Sustituir a los empleados por sistemas de inteligencia artificial.

Respuesta correcta: C

3. ¿Cuál de las siguientes opciones se considera un «factor de riesgo digital» específico en el sector turístico?

- A. Una inundación en la recepción del hotel.
- B. La inestabilidad política en un país de origen de los turistas.
- C. El pirateo de páginas web de reservas o el robo de datos de clientes.
- D. Un cambio en las preferencias de los consumidores hacia el turismo rural.

Respuesta correcta: C

4. ¿Qué es un «sistema de alerta temprana» en el contexto de esta unidad?

- A. Una alarma sonora que indica que hay un incendio en el edificio.
- B. Indicadores y señales que permiten detectar la escalada de una crisis antes de que se vuelva incontrolable.
- C. Un sistema de mensajes automatizados para dar la bienvenida a los clientes.
- D. Un informe trimestral sobre los resultados financieros de la empresa.

Respuesta correcta: B

5. En una matriz de riesgos, si un evento tiene una «probabilidad alta» y un «impacto crítico», ¿qué medida debería priorizarse?

- A. Ignorar el riesgo porque es demasiado complejo de gestionar.
- B. Supervisar el riesgo de forma pasiva una vez al año.
- C. Aplicar medidas de mitigación inmediatas y planes de respuesta.
- D. Delegar la responsabilidad exclusivamente en proveedores externos.

Respuesta correcta: C

6. Basándonos en el caso real de Meliá Hotels (2021), ¿qué característica define su respuesta como «resiliente»?

- A. El pago inmediato del rescate a los ciberdelincuentes para evitar la mala prensa.
- B. La capacidad de aislar los sistemas y utilizar copias de seguridad para mantener la continuidad del negocio.
- C. El cierre total de la cadena hotelera hasta que el virus desapareciera por sí solo.
- D. La negación pública del ataque para no alarmar a los inversores.

Respuesta correcta: B

7. Según la teoría de la Organización de Alta Fiabilidad (HRO), ¿quién suele estar en mejor posición para detectar las vulnerabilidades del día a día?

- A. Los auditores externos que visitan la empresa anualmente.
- B. El personal de primera línea que maneja los sistemas a diario.
- C. Los accionistas de la empresa que analizan los resultados financieros.
- D. El departamento de marketing a través de las redes sociales.

Respuesta correcta: B

8. En el ciclo de vida de una crisis, ¿qué fase se produce inmediatamente después de la «respuesta»?

- A. Prevención.
- B. Preparación.
- C. Recuperación.
- D. Mitigación.

Respuesta correcta: C

9. ¿Cuál es el objetivo principal de un ejercicio de «mapeo de riesgos» para una agencia de viajes?

- A. Crear un folleto publicitario con los mejores destinos del mundo.
- B. Identificar vulnerabilidades y evaluar la probabilidad de amenazas específicas.
- C. Elaborar un mapa de las salidas de emergencia de la oficina física.
- D. Calcular el tiempo que tardan los empleados en llegar a su lugar de trabajo.

Respuesta correcta: B

10. ¿Qué habilidad demuestra un estudiante que sabe cómo comunicar los riesgos a «partes interesadas sin conocimientos técnicos»?

- A. La capacidad de escribir código avanzado para detener un virus.
- B. La capacidad de explicar una amenaza técnica de forma comprensible para la toma de decisiones.
- C. El dominio de varios idiomas para ayudar a los turistas extranjeros.
- D. La capacidad de redactar contratos legales complejos sin la ayuda de abogados.

Respuesta correcta: B

2.2 Resiliencia y transiciones gemelas (verde y digital)

Al finalizar esta subunidad, los alumnos serán capaces de aplicar los ODS a las operaciones turísticas, identificar sinergias verdes y digitales, evaluar soluciones inteligentes para mejorar la resiliencia y colaborar con las autoridades públicas y los proveedores de tecnología.

- El impacto del cambio climático en el turismo (olas de calor, escasez de agua, cambios en la estacionalidad)
- Integración de los Objetivos de Desarrollo Sostenible (ODS) de las Naciones Unidas y de los principios de la economía circular en los modelos turísticos.
- Tecnologías inteligentes en el turismo (destinos turísticos inteligentes, sensores del Internet de las cosas —energía, agua, ocupación—, inteligencia artificial para la previsión de la demanda y la respuesta ante crisis)
- Marco europeo: Pacto Verde de la UE, Estrategia Digital de la UE e inclusión.

Actividad práctica sugerida:

- Estudio de caso de un destino turístico inteligente en Europa

El eje central de esta unidad es la **convergencia estratégica** entre la sostenibilidad medioambiental y la transformación digital, un proceso conocido en el marco europeo como la «transición **doble**». El objetivo no es simplemente que los profesionales del turismo utilicen herramientas digitales o reciclen residuos, sino que aprendan a utilizar la tecnología avanzada como motor de la sostenibilidad y, a su vez, garanticen que dicha tecnología sea resiliente ante las amenazas medioambientales.

Esta unidad se divide en tres subunidades:

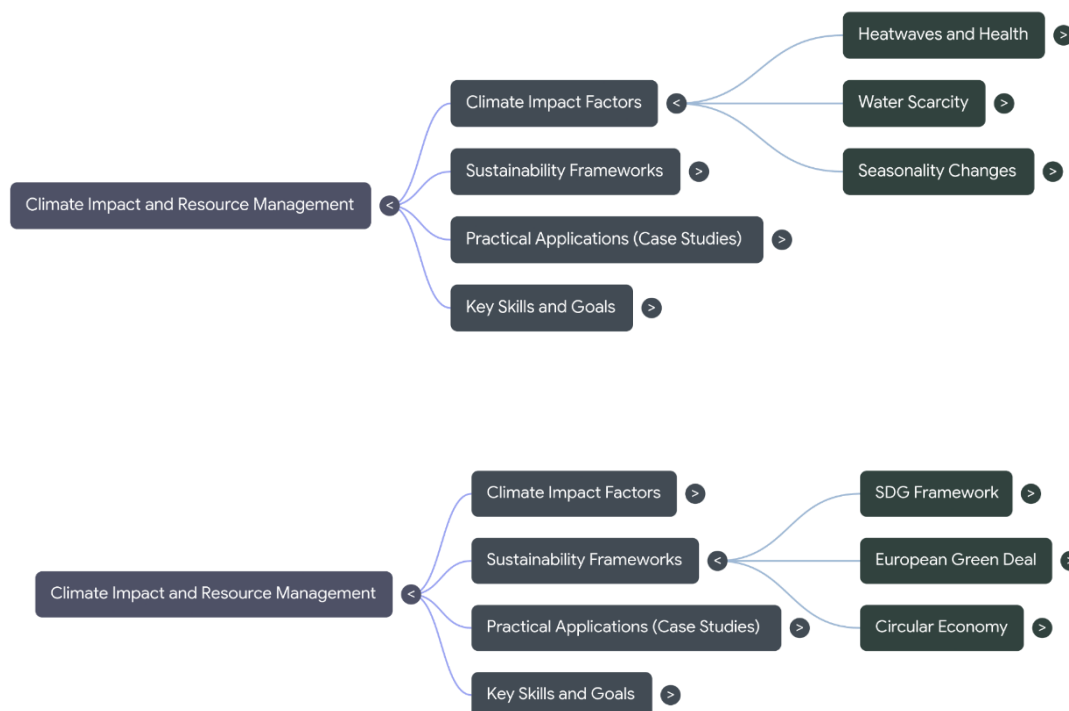
1. Impacto climático y gestión de recursos.
2. Tecnologías inteligentes (Smart Tech) para la resiliencia.
3. El marco europeo y los destinos inteligentes.

2.2.1 Impacto climático y gestión de recursos (2 horas)

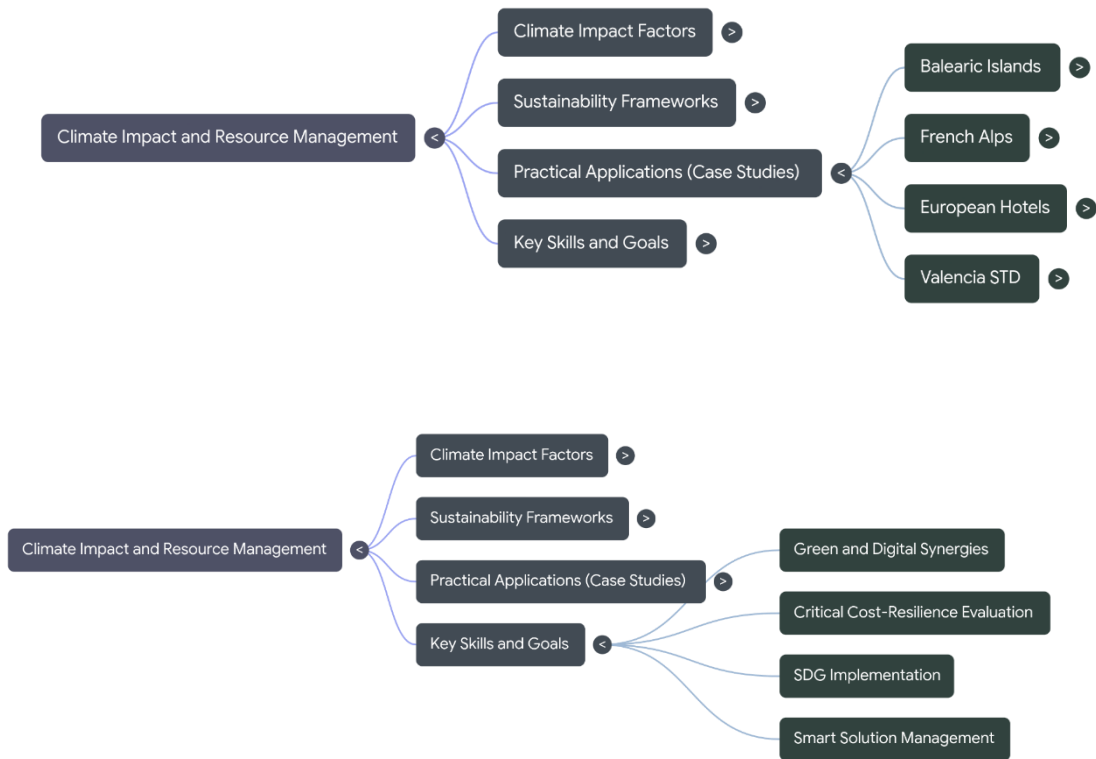
El punto de partida es reconocer que el cambio climático no es una amenaza lejana, sino un factor que ya está alterando las operaciones turísticas a través de **olas de calor, escasez de agua y cambios drásticos en la estacionalidad**.

- **Enfoque práctico:** los estudiantes dejarán de considerar el clima como una variable incontrolable y, en su lugar, lo analizarán como un factor de riesgo que puede gestionarse mediante datos.
- **Sostenibilidad integrada:** Exploramos la aplicación de los **Objetivos de Desarrollo Sostenible (ODS)** y los principios de la **economía circular**. Esto implica transformar el modelo de negocio, pasando de uno de «consumo y desecho» a uno de «eficiencia y regeneración».

Esquema de la unidad



Unidad formativa I: Resiliencia en el Turismo



1. Contenidos teóricos (1 hora)

1. Impacto climático: datos y realidad operativa:

El impacto del cambio climático en el turismo no es una proyección de futuro, sino una realidad que está alterando la oferta y la demanda actuales.

- **Olas de calor y salud:** Según informes de la Agencia Europea de Medio Ambiente, el aumento de las temperaturas extremas está reduciendo el atractivo de los destinos del sur de Europa durante el verano, lo que desplaza la demanda hacia el norte o hacia las temporadas intermedias (primavera/otoño).
- **Escasez de agua:** En destinos insulares o mediterráneos, la escasez de agua se está convirtiendo en un riesgo operativo crítico. La teoría de la gestión de los recursos hídricos sostiene que el turismo consume una cantidad de agua por persona significativamente mayor que la población local, lo que hace necesaria la implantación de tecnologías de medición (IoT) para evitar conflictos sociales y garantizar la continuidad operativa.
- **Cambios en la estacionalidad:** La pérdida de previsibilidad climática afecta a la planificación financiera y de personal de las empresas turísticas.

2. El impacto climático y el marco de los ODS

Este pilar incorpora los Objetivos de Desarrollo Sostenible (concretamente los ODS 12 y 13) como brújula para reforzar la resiliencia.

- **ODS 12 (Consumo y producción responsables):** Se basa en la teoría del «ciclo de vida». Las empresas deben supervisar sus cadenas de suministro para reducir los residuos.
- **ODS 13 (Acción por el clima):** subraya la necesidad de contar con planes de mitigación y adaptación al cambio climático en las organizaciones turísticas.
- **Alineación con el Pacto Verde Europeo:** este marco tiene como objetivo convertir a Europa en el primer continente climáticamente neutro para 2050. El turismo resiliente debe cumplir con la normativa sobre eficiencia energética y reducción de emisiones para seguir siendo competitivo y poder optar a la financiación de la UE.

El cambio climático (olas de calor, escasez de agua) se analiza como un factor de riesgo que puede gestionarse mediante datos y los principios de la economía circular.

3. La teoría de la economía circular aplicada al turismo

La economía circular es el antídoto contra la vulnerabilidad de la cadena de suministro.

- **El modelo de las «3 R»:** Reducir, Reutilizar y Reciclar. En el turismo, esto se traduce en la eliminación de los plásticos de un solo uso, la gestión eficiente de los residuos orgánicos y el diseño de edificios hoteleros con materiales sostenibles.
- **Resiliencia de los insumos:** al circularizar los recursos, la empresa es menos vulnerable a las fluctuaciones externas de los precios o a las interrupciones del suministro a nivel mundial.
- **Sostenibilidad real:** La UE está promoviendo el Plan de Acción para la Economía Circular, que exige a las industrias (incluido el turismo) que rediseñen sus procesos para mantener el valor de los productos y materiales durante el mayor tiempo posible.

2. Competencias desarrolladas en la unidad

Una vez dominada esta teoría, el estudiante será capaz de:

1. **Evaluar soluciones inteligentes** de los proveedores de tecnología desde una perspectiva crítica de resiliencia de costes.
2. **Identificar sinergias** en las que una inversión digital reduzca también el impacto medioambiental.
3. **Colaborar con expertos** técnicos para garantizar que la transición ecológica no deje puertas traseras para los ciberdelincuentes.

3. Casos prácticos (1 hora)

- I. **Caso práctico 1:** Gestión de la escasez de agua en las Islas Baleares (Teoría: El agua y el IoT)

- **Contexto real:** En los destinos insulares del Mediterráneo, la escasez de agua es un riesgo crítico que afecta a la resiliencia. El consumo de los turistas suele ser tres veces superior al de los residentes locales.
- **Aplicación práctica:** Las principales cadenas hoteleras (como Iberostar o Meliá) han implantado **sensores de agua basados en el IoT** para supervisar el consumo en tiempo real y detectar fugas ocultas de forma inmediata.

A través de este caso práctico, podemos evaluar soluciones inteligentes para mejorar la resiliencia y el uso de tecnologías para gestionar la escasez de agua.



Gestión de la escasez de agua en las Islas Canarias

II. **Caso 2:** Adaptación a la estacionalidad en los Alpes franceses (Teoría: Clima y estrategia)

- **Contexto real:** Debido a las olas de calor y a la falta de nevadas constantes, las estaciones de esquí están experimentando **cambios en la estacionalidad**.
- **Aplicación práctica:** Destinos como Chamonix están diversificando su modelo hacia el «turismo de cuatro estaciones», utilizando **la IA para pronosticar la demanda** relacionada con el clima y rediseñando su oferta para incluir rutas de senderismo guiadas digitalmente cuando no hay nieve.

Este caso se ajusta a la identificación de sinergias ecológicas y digitales y a la aplicación de los principios de resiliencia ante el cambio climático.



En los Alpes, el cambio climático está convirtiendo los glaciares en lagos • FRANCE 24 English

III. **Caso 3:** Iniciativa «Cero residuos» en hoteles europeos (Teoría: economía circular y ODS)

- **Contexto real:** La gestión de residuos es un pilar de la economía circular. Un hotel medio genera toneladas de residuos alimentarios y plásticos de un solo uso.
- **Aplicación práctica:** Los hoteles que han adoptado los ODS de la ONU (concretamente el ODS 12) utilizan plataformas digitales para medir los residuos de cocina y redistribuir el excedente de comida a través de aplicaciones (como «Too Good To Go»), aplicando los principios de la circularidad.

El objetivo es demostrar la capacidad de aplicar los ODS a las operaciones turísticas y colaborar con los proveedores de tecnología.

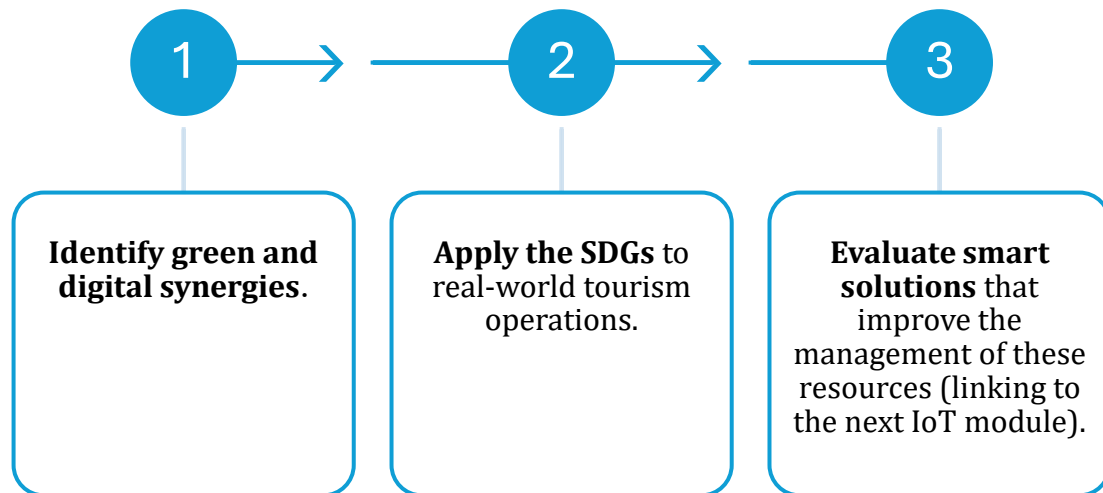
IV. **Caso 4:** Seguimiento de las emisiones de carbono en Valencia, una ciudad STD (Teoría: Pacto Verde Europeo y Estrategia Digital)

- **Contexto real:** Valencia es un **destino turístico inteligente** que mide la huella de carbono de su actividad turística.
- **Aplicación práctica:** Aprovechando la **Estrategia Digital de la UE**, la ciudad integra datos sobre transporte, energía y agua para ofrecer transparencia climática, en consonancia con el **Pacto Verde de la UE**.

Esto permite realizar un estudio de caso sobre un destino turístico inteligente en Europa, tal y como se sugiere en las actividades prácticas del programa.

Aplicación práctica de los conocimientos

Para que el alumno demuestre su competencia en esta área, el curso exige que sea capaz de:



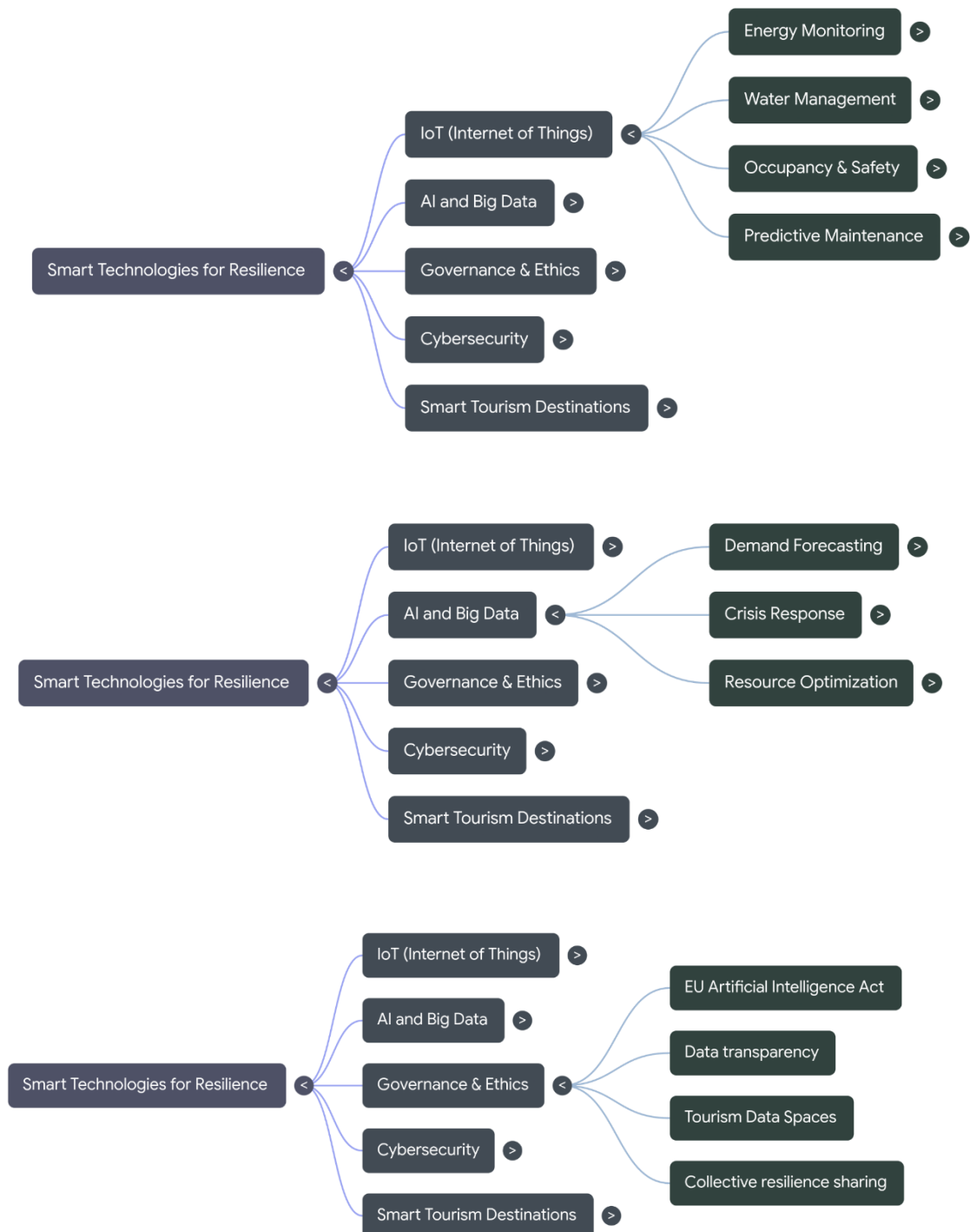
2.2.2 Tecnologías inteligentes (SmartTech) para la resiliencia (2,5 horas)

El objetivo teórico es capacitar a los estudiantes para evaluar e implementar soluciones inteligentes que mejoren la gestión de crisis y la sostenibilidad.

El módulo plantea que la tecnología es la herramienta indispensable para alcanzar los objetivos medioambientales. No hay sostenibilidad real sin medición, y no hay medición eficiente sin digitalización.

- **Tecnologías inteligentes:** se exploran soluciones como **los sensores del Internet de las cosas (IoT)** para la monitorización en tiempo real del consumo de energía y agua, así como el uso de **la inteligencia artificial (IA)** para predecir la demanda y optimizar los recursos, reduciendo así la huella de carbono. **Destinos inteligentes:** se introduce el concepto de **destinos turísticos inteligentes**,
- en los que se fomenta la resiliencia a través de una infraestructura digital compartida que permite una respuesta rápida ante crisis climáticas o sanitarias.

Resumen de la unidad





1. Contenidos teóricos que se impartirán (1,5 horas)

IoT (Internet de las cosas): los ojos del negocio

El IoT se define como la red de objetos físicos interconectados que recopilan y comparten datos en tiempo real. En el turismo resiliente, estos sensores eliminan la «ceguera operativa».

- **Monitorización energética:** sensores inteligentes que detectan picos anómalos en el consumo, lo que ayuda a prevenir fallos en la red eléctrica o incendios eléctricos.
- **Gestión del agua:** dispositivos que miden el caudal de agua y detectan inmediatamente fugas invisibles, protegiendo el recurso en zonas de escasez.

- **Niveles de ocupación:** uso de sensores de presencia o mapas de calor para optimizar la climatización y la seguridad física, evitando aglomeraciones peligrosas.
- **Mantenimiento predictivo:** pasar de reparar lo que está averiado a prevenir las averías antes de que se produzcan, garantizando la continuidad del negocio.

IA y big data: el cerebro de la respuesta ante crisis

Si el IoT son los «ojos», la Inteligencia Artificial (IA) es la capacidad de **predecir y tomar decisiones** basadas en esos datos.

- **Previsión de la demanda:** modelos de IA que analizan datos históricos y tendencias meteorológicas para predecir la ocupación, optimizando la adquisición de suministros y reduciendo el desperdicio de alimentos.
- **Respuesta ante crisis:** algoritmos que procesan señales de «alerta temprana» (EWS) para activar automáticamente protocolos de emergencia (por ejemplo, alertas a los huéspedes en caso de incendio o inundación).
- **Optimización de recursos críticos:** la IA puede gestionar microrredes para dar prioridad al suministro eléctrico a áreas vitales (como la refrigeración de alimentos o los sistemas de seguridad) durante un corte parcial de suministro.

Ética y responsabilidad en la IA

Uso ético y responsable de la IA de conformidad con la Ley de Inteligencia Artificial de la UE. Se centra en la transparencia en el tratamiento de los datos biométricos y en la eliminación de los algoritmos de predicción de la demanda para garantizar una respuesta equitativa ante las crisis.

- **Espacios de datos turísticos**

Introducción a los espacios de datos turísticos. Esta teoría explica cómo las empresas pueden compartir de forma segura indicadores de riesgo e información sobre sostenibilidad con la competencia y las autoridades públicas. El objetivo es reforzar la resiliencia colectiva del destino mediante el intercambio de datos en tiempo real (por ejemplo, alertas sobre el exceso de afluencia o el consumo de recursos) sin comprometer los secretos comerciales ni la privacidad de los clientes.

Ciberseguridad en la doble transición: protección de la infraestructura verde

La integración de tecnologías verdes (sensores de agua, paneles solares inteligentes, control climático automatizado) crea nuevos vectores de ataque. Una empresa no puede ser sostenible si no es **segura desde el punto de vista digital**.

1. **La amenaza de la interconectividad:** si se piratea un sensor de agua, un atacante podría provocar inundaciones deliberadas o cortes en el suministro, lo que afectaría a la salud y a la resiliencia operativa.
2. **Protección de la infraestructura crítica:** Los alumnos deben comprender que la ciberseguridad debe aplicarse no solo al ordenador de recepción, sino a todos los sensores conectados (seguridad desde el diseño).
3. **Confianza y reputación:** En la era digital, perder el control sobre los sistemas inteligentes de un hotel destruye la confianza de los clientes y la viabilidad del negocio.

2. Competencias desarrolladas en la unidad

Al completar este módulo, el alumno habrá desarrollado las siguientes competencias profesionales:

- **Evaluación técnica de soluciones de IoT:** capacidad para identificar e implementar sensores de monitorización (energía, agua, ocupación) que eliminen los puntos ciegos operativos y permitan el mantenimiento predictivo.
- **Gestión proactiva mediante IA y big data:** capacidad para utilizar modelos de previsión de la demanda y sistemas de alerta temprana (EWS) con el fin de optimizar los recursos y automatizar la respuesta ante situaciones de crisis.
- **Aplicación de los principios de «ciberseguridad desde el diseño»:** capacidad para proteger la infraestructura verde (sensores, sistemas de gestión de edificios [BMS], sistemas de climatización [HVAC]) mediante la segmentación de la red y el cumplimiento de marcos normativos como la Directiva NIS2.
- **Gobernanza de datos ética y colaborativa:** Competencia para gestionar los datos de forma transparente, de conformidad con el Reglamento de la UE

sobre IA, y para participar en los «Espacios de Datos Turísticos» con el fin de reforzar la resiliencia colectiva.

3. Casos concretos (1 hora)

Caso de uso 1: IoT (Los ojos de la empresa)

El **IoT** permite pasar de una gestión reactiva («se ha estropeado») a una gestión proactiva («va a fallar»).

1. Caso real: NH Hotel Group e Iberostar (Eficiencia y prevención).

- **Contexto:** Estas cadenas utilizan sistemas de gestión de edificios (BMS) con sensores de IoT para supervisar el consumo de agua y energía en tiempo real.
- **Resiliencia aplicada:** en caso de una fuga de agua invisible en una tubería principal a las 3:00 de la madrugada, el sensor detecta el caudal anómalo y corta automáticamente el suministro o envía una alerta inmediata. Esto evita graves daños estructurales y el cierre de habitaciones, salvaguardando la continuidad del negocio.

2. Ejemplo del mundo real: Sensores de ocupación en zonas comunes.

- **Contexto:** Uso de sensores de calor o pings de Wi-Fi para medir la densidad de personas en balnearios o restaurantes.
- **Resiliencia aplicada:** En el contexto de crisis sanitarias o evacuaciones, esto permite a los responsables saber exactamente dónde se están concentrando las multitudes y reubicar de forma segura al personal o a los clientes.

Caso de uso 2: IA y big data (el cerebro)

La **IA** procesa el «ruido» de los datos para ofrecer predicciones precisas que ahorran recursos.

1. Ejemplo real: Benidorm o Venecia (salas de control inteligentes).

- **Contexto:** Como **destinos turísticos inteligentes**, utilizan el big data (datos de teléfonos, cámaras y redes sociales) y la IA para predecir la ocupación.

- **Resiliencia aplicada:** si la IA detecta un pico de ocupación excesivo combinado con una alerta de ola de calor, el destino puede activar protocolos para reforzar los servicios sanitarios y de transporte antes de que se produzca un colapso.

2. Ejemplo real: Winnow Solutions (IA contra el desperdicio alimentario).

- **Contexto:** Los hoteles y los cruceros utilizan cámaras con IA en las cocinas para analizar qué alimentos se tiran a la basura.
- **Resiliencia operativa:** La IA identifica patrones (por ejemplo, «siempre tiramos el 30 % del arroz los martes»). Esto nos permite ajustar las compras, reduciendo así los costes y alineándonos con el ODS 12 sobre producción y consumo responsables.

Caso práctico 3: Ciberseguridad (proteger el escudo verde)

La ciberseguridad es esencial para una transición digital fiable.

1. Caso de «alerta»: el hackeo del termómetro del acuario.

- **Contexto:** En un casino de EE. UU., unos atacantes se infiltraron en la red corporativa a través de un termómetro inteligente (IoT) situado en el acuario del vestíbulo.
- **Lección de resiliencia:** Este caso real sirve para enseñar a los alumnos que cada sensor de agua o energía instalado con fines «ecológicos» es un posible punto de entrada. La resiliencia requiere la segmentación de la red: los datos de los sensores de agua nunca deben estar en la misma red que los datos de las tarjetas de crédito de los clientes.

2. Caso real: Aplicación de la Directiva NIS2 en cadenas hoteleras.

- **Contexto:** Los hoteles europeos están reforzando la seguridad de sus sistemas de gestión de edificios (climatización, iluminación) para cumplir con el marco normativo de la UE.
- **Resiliencia aplicada:** Al proteger los sistemas de climatización, se evita que un ciberdelincuente tome el control del aire acondicionado durante una ola de calor, lo que obligaría a evacuar el hotel y provocaría una crisis de reputación de gran envergadura.

2.2.3 El marco europeo y los destinos inteligentes (2,5 horas)

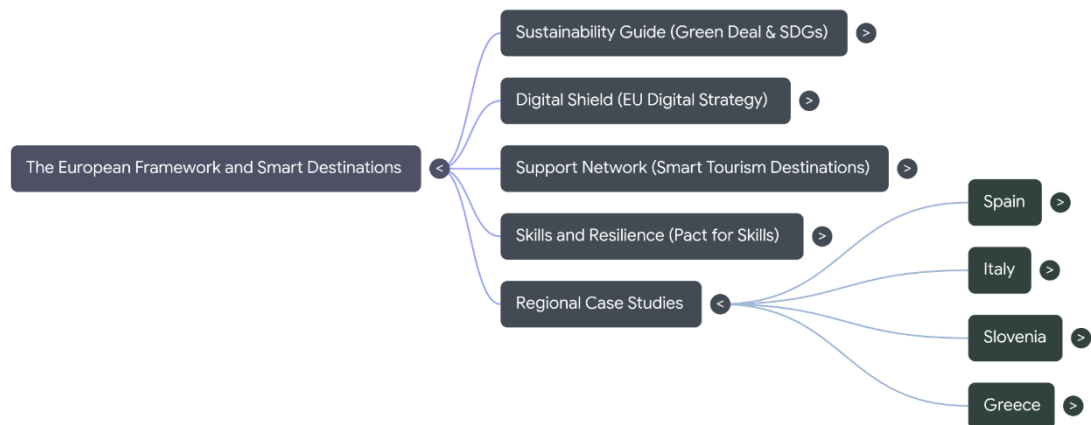
Este módulo no trata de leyes lejanas, sino de cómo la Unión Europea contribuye a que tu negocio sea más moderno y seguro. Aprenderemos que conceptos como el **Pacto Verde de la UE** o la **Estrategia Digital** son, en realidad, «sellos de calidad» y guías de supervivencia.

Cuando un hotel decide dejar de imprimir folletos y utiliza un código QR, o cuando una oficina de turismo utiliza una aplicación para avisar de que una playa está llena, están aplicando estas políticas europeas. El objetivo aquí es que el alumno comprenda que ser un «destino inteligente» implica utilizar la información de la que ya disponemos para garantizar que los turistas estén más seguros y que se cuide mejor el medio ambiente.

Esquema de la unidad



Unidad formativa I: Resiliencia en el Turismo



1. Contenidos teóricos (1 hora)

Para facilitar el aprendizaje, hemos dividido la teoría en tres conceptos operativos que los alumnos deben conocer:

I. La Guía de Sostenibilidad (Pacto Verde y ODS)

- **Qué es:** un compromiso de las empresas para contaminar menos y ahorrar más.
- **En la práctica diaria:** esto significa dar prioridad a los proveedores locales, reducir el uso de plástico y utilizar la energía de forma eficiente.
- **Resiliencia:** si consumes menos electricidad y agua, tu empresa es más resiliente ante las subidas de precios y las sequías.

II. El Escudo Digital (Estrategia Digital de la UE)

- **Qué es:** Normas para hacer de Internet un lugar seguro para las empresas y los clientes.
- **En la práctica:** Significa proteger los datos de los clientes y utilizar herramientas digitales que no fallen.
- **Resiliencia:** El personal capaz de detectar un correo electrónico de phishing protege el dinero y la reputación de la empresa.

III. La red de apoyo (Destinos Turísticos Inteligentes – STD)

- **Qué es:** Destinos que comparten datos para ayudar a todo el mundo.
- **En la vida cotidiana:** Consultar la web oficial de la ciudad para ver las previsiones de afluencia de público o las alertas meteorológicas.
- **Resiliencia:** Saber cómo actuar antes de que surja el problema (por ejemplo, advertir a un grupo de que no vaya a una zona debido a una alerta por ola de calor).

1. Competencias desarrolladas en esta unidad

Al finalizar este módulo, el alumno será capaz de:

- **Alinear la estrategia empresarial con las políticas europeas:** comprender y aplicar el *Pacto Verde Europeo* y la *Estrategia Digital de la UE* como guías de supervivencia y «sellos de calidad» para la modernización empresarial.

- **Operar según el modelo de Destino Turístico Inteligente (STD):** utilizar infraestructuras de datos compartidas y herramientas tecnológicas para mejorar la seguridad de los turistas y la protección del medio ambiente.
- **Implementar medidas de resiliencia verde y digital:** digitalizar los procesos operativos (como el uso de códigos QR o menús digitales) para reducir costes, ahorrar recursos y cumplir con las normas de sostenibilidad de la UE.
- **Gestionar la ciberseguridad y la privacidad de los datos:** aplicar el «Escudo Digital» para proteger los datos de los clientes y detectar amenazas como *el phishing*, salvaguardando así la reputación de la organización.
- **Fomentar el aprendizaje continuo y la colaboración regional:** participar en marcos de cooperación como el *Pacto por las Competencias* para garantizar que el capital humano sea la principal defensa frente a las crisis tecnológicas.

2. Casos concretos por región (1,5 horas)

I. España

A. Caso 1: El programa «Menorca sin plástico»

- **Contexto:** Pacto Verde de la UE y ODS 12 (Consumo responsable).
- **Acción:** Los pequeños hoteles y las empresas locales están sustituyendo las botellas de plástico por dispensadores de agua filtrada y códigos QR para las guías turísticas.
- **Aplicación para el alumno:** El alumno aprende que la digitalización de la información (códigos QR en lugar de papel) es una medida de resiliencia ecológica que ahorra costes y cumple con la normativa de la UE.



[Alianza «Menorca sin Plástico» \(ENG\)](#)

B. **Caso 2:** El curso TREADS (Pacto por las Competencias)

- **Marco:** Pacto por las Competencias.
- **Acción:** El curso que están realizando los alumnos es un ejemplo real de este pacto europeo para garantizar que los trabajadores no se queden atrás en materia tecnológica.
- **Aplicación para el alumno:** Comprender que su formación es una herramienta para la resiliencia. Un trabajador cualificado es la mejor defensa de una empresa frente a cualquier crisis.

C. **Caso 3:** Gestión de residuos «sin desbordamientos» (Santander, España)

- **El problema:** Durante la temporada alta, las papeleras de las zonas turísticas se llenan rápidamente, lo que genera desorden y da una mala imagen.
- **La acción «inteligente»:** El ayuntamiento instaló sensores en las papeleras que avisan al servicio de limpieza solo cuando están al 80 % de su capacidad.
- **Relación con el marco europeo:**
 - **Estrategia Digital de la UE:** uso de datos y del Internet de las cosas (IoT) para mejorar un servicio público.
 - **Pacto Verde Europeo:** Se ahorra combustible al no enviar camiones de recogida de residuos a vaciar las papeleras.

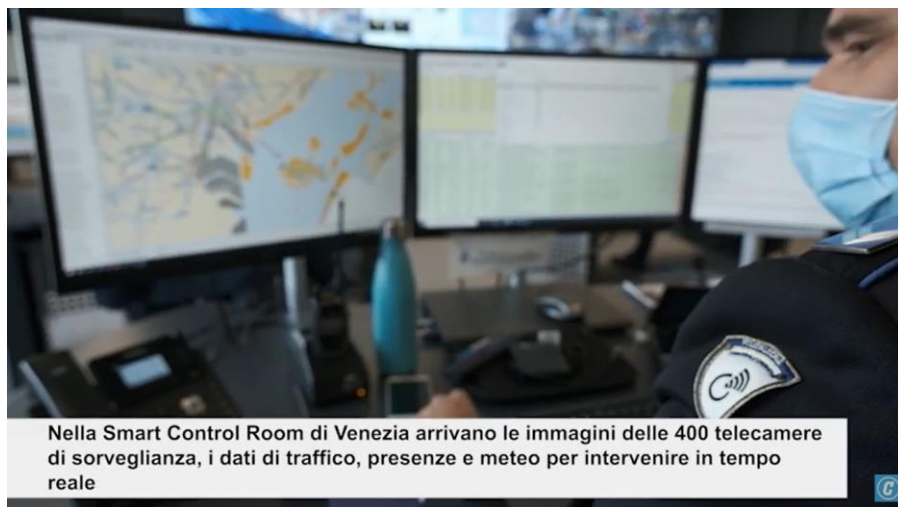
- **Resiliencia para los estudiantes:** si trabajas en un punto de información, puedes identificar qué zonas están limpias y bien cuidadas para recomendarlas, evitando así las quejas de los turistas por la falta de higiene.
- D. **Caso 4:** El sistema de «semáforos» de ocupación de la playa (Benidorm, España)
- **El problema:** El exceso de aforo en una playa plantea riesgos de seguridad, provoca estrés térmico y da lugar a una mala experiencia del cliente.
 - **La solución «inteligente»:** Una sencilla aplicación web muestra en tiempo real si la playa está en verde (libre), amarillo (moderada) o rojo (llena).
 - **Relación con el marco europeo:**
 - **Destino turístico inteligente (STD):** uso de la tecnología para gestionar el flujo de personas de forma segura.
 - **Inclusión:** Permite a las personas con movilidad reducida elegir horarios menos concurridos para visitar la playa de forma segura.
 - **Resiliencia para el estudiante:** Un recepcionista de hotel puede consultar la página web e informar al cliente: «No vayas ahora a la playa de Levante, la IA indica que está llena; prueba mejor con esta otra cala, que es más segura».
- E. **Caso 5:** Formación en ciberseguridad para guías (Pacto por las Competencias)
- **El problema:** Los guías autónomos suelen utilizar redes Wi-Fi públicas para gestionar las reservas de sus clientes, lo que los expone al robo de datos.
 - **La acción «inteligente»:** Un programa de formación local (como este curso de TREADS) enseña a los guías a utilizar redes seguras y a proteger los datos de los turistas.
 - **Vínculo con el marco europeo:**

- **Pacto por las Competencias:** inversión en las competencias digitales de los trabajadores para garantizar que no se queden atrás.
- **Estrategia Digital de la UE:** Protección de la privacidad y los datos en el espacio digital europeo.
- **Resiliencia del alumno:** El alumno comprende que su propia formación es lo que le hace resiliente: saber qué redes debe evitar protege su negocio y la confianza de sus clientes.

II. Italia

A. Caso 1: La «sala de control inteligente» de Venecia

- **El problema:** La extrema masificación en Venecia genera riesgos para la seguridad, deteriora la experiencia turística y ejerce presión sobre los servicios de emergencia en un entorno geográfico complejo.
- **La acción «inteligente»:** un centro de control avanzado que integra datos procedentes de sensores, señales de teléfonos móviles, cámaras con inteligencia artificial y el GPS de los vaporettos para supervisar el flujo y la densidad de personas en tiempo real.
- **Relación con el marco europeo:**
 - **Destino Turístico Inteligente (STD):** uso de tecnología de vanguardia para la gestión segura de la capacidad de acogida del destino.
- **Resiliencia para el visitante:** El director de un hotel puede recibir alertas de masificación en zonas concretas (como la plaza de San Marcos) y recomendar a sus huéspedes rutas alternativas o museos menos concurridos, evitando así situaciones estresantes y mejorando la seguridad.



Dentro de la sala de control inteligente de Venecia

B. **Caso 2:** Movilidad sostenible en los Dolomitas (South Tyrol Guest Pass)

- **El problema:** La dependencia de los coches particulares en los valles alpinos provoca atascos, contaminación en ecosistemas frágiles y vulnerabilidad ante los deslizamientos de tierra que bloquean las carreteras.
- **La acción «inteligente»:** La digitalización completa del transporte público a través del «Guest Pass», que permite a los turistas utilizar trenes y autobuses de montaña de forma gratuita y sin límites, integrando reservas digitales para servicios de lanzadera a lugares clave de gran altitud.
- **Relación con el marco europeo:**
 1. **Pacto Verde de la UE:** Reducción drástica de la huella de carbono del transporte turístico en las zonas protegidas.
- **Resiliencia para el estudiante:** El estudiante aprende que facilitar la movilidad verde digitalizada no solo es sostenible, sino que también reduce el riesgo operativo de que los clientes queden atrapados en atascos o en carreteras secundarias bloqueadas.

C. **Caso práctico 3:** Gestión del agua basada en el IoT en hoteles de la Costa Amalfitana

- **El problema:** La escasez de agua y el terreno escarpado dificultan garantizar un suministro estable de agua en verano, lo que supone un

riesgo crítico para la higiene y la satisfacción de los clientes en los hoteles de lujo.

- **La acción «inteligente»:** Instalación de sensores de IoT en las tuberías y depósitos de los hoteles para detectar fugas invisibles y supervisar el consumo en tiempo real.
- **Relación con el marco europeo:**
 - **ODS 6 y 12:** Gestión eficiente del agua y consumo responsable.
- **Resiliencia para el estudiante:** Ante una anomalía en el caudal a las 4:00 de la madrugada, el sistema avisa al recepcionista, lo que permite reparar una fuga antes de que se vacíe el depósito de reserva del hotel, garantizando así la continuidad del servicio.

D. **Caso 4:** «Feel Florence» – Aplicación de la diversificación digital

- **El problema:** El centro histórico de Florencia sufre un desgaste excesivo de su patrimonio, mientras que otros barrios artísticos cercanos no reciben visitantes, lo que afecta a la resiliencia social y económica del destino.
- **La acción «inteligente»:** Una aplicación oficial que utiliza datos en tiempo real para sugerir itinerarios menos concurridos y experiencias fuera de los circuitos habituales en función del perfil del turista.
- **Relación con el marco europeo:**
 - **Estrategia Digital de la UE:** uso ético de los datos de comportamiento para mejorar la convivencia entre residentes y turistas.
- **Resiliencia para el estudiante:** un guía o un recepcionista puede utilizar la aplicación para mostrar al cliente que visitar un barrio periférico es una opción más cómoda y «más segura» en comparación con las interminables colas del centro de la ciudad.



Feel Florence

III. Eslovenia

A. Caso 1: El Programa de Turismo Verde de Eslovenia (GSST)

- **El problema:** Garantizar que todas las partes interesadas del sector (hoteles, destinos, agencias) cumplan con auténticos estándares de sostenibilidad para evitar el «greenwashing» y mejorar la eficiencia en el uso de los recursos.
- **La acción «inteligente»:** Una plataforma digital nacional que unifica los criterios de sostenibilidad y las herramientas de medición bajo una única marca. Permite a las empresas supervisar su consumo de energía y agua para obtener certificaciones oficiales.
- **Vínculo con el marco europeo:**
 - **Pacto Verde de la UE y ODS 12:** Utilizar la tecnología para promover patrones de consumo y producción responsables.
- **Resiliencia para el estudiante:** El estudiante comprende que operar bajo un marco nacional de sostenibilidad digital reduce los costes operativos y hace que la empresa sea más resiliente ante las crisis de los precios de la energía.



[Eslovenia Verde](#)  [La historia de la Eslovenia verde.](#)

B. **Caso 2:** Gestión de la movilidad alpina en los valles de Bohinj y Bled

- **El problema:** La saturación de vehículos privados en los valles alpinos y en los alrededores de los lagos degrada el medio ambiente, genera ruido y dificulta el acceso de los servicios de emergencia.
- **La acción «inteligente»:** Implantación de sistemas de reserva digital para aparcamientos situados fuera de la ciudad y uso de autobuses lanzadera controlados mediante GPS y aplicaciones para turistas.
- **Relación con el marco europeo:**
 - **Destino Turístico Inteligente (STD):** gestión tecnológica de los flujos de visitantes para proteger el patrimonio natural.
- **Resiliencia para los estudiantes:** Un recepcionista de un hotel de montaña puede comprobar la ocupación del aparcamiento en tiempo real y aconsejar a los huéspedes que utilicen opciones de transporte digital, evitando así la congestión del tráfico en el destino debido a la masificación.

C. **Caso 3:** Monitorización digital del microclima en la cueva de Postojna

- **El problema:** El ecosistema kárstico es extremadamente frágil; incluso pequeños cambios en la temperatura o en los niveles de CO₂ provocados por un número excesivo de visitantes pueden dañar las formaciones y la fauna endémica.
- **La acción «inteligente»:** uso de sensores avanzados de IoT que supervisan en tiempo real las condiciones biológicas y

microclimáticas de la cueva, enviando alertas si los niveles se desvían de los límites de seguridad.

- **Relación con el marco europeo:**

- **Transición doble:** la tecnología digital (sensores) al servicio de un objetivo ecológico fundamental (la protección de la biodiversidad).

- **Resiliencia para los estudiantes:** Aprender a reconocer las «señales de alerta temprana» medioambientales que requieren ajustar los flujos turísticos para garantizar la supervivencia a largo plazo del recurso turístico.

D. **Caso 4:** Infraestructura de datos de las ETI para la toma de decisiones

- **El problema:** La falta de datos actualizados y compartidos impedía dar respuestas rápidas a perturbaciones externas (como pandemias o desastres naturales).

- **La acción «inteligente»:** Creación de un centro de datos de turismo digital que centralice la información estadística y operativa para los ciudadanos y las empresas.

- **Relación con el marco europeo:**

- **Estrategia Digital de la UE:** uso de infraestructuras de datos para mejorar la gobernanza y la capacidad de respuesta ante crisis.

- **Resiliencia para el alumno:** El experto resiliente utiliza este centro para seguir las tendencias de digitalización y sostenibilidad en su ámbito, lo que le permite adaptarse de forma proactiva a la demanda.

IV. Grecia

A. **Caso 1:** Gestión digital de cruceros en Santorini

- **El problema:** El ataque simultáneo de varios cruceros de gran capacidad satura el puerto y las calles de Fira, lo que deteriora la experiencia de los visitantes y genera riesgos de seguridad en un destino geológicamente frágil.

- **La acción «inteligente»:** Implantación de un sistema digital de gestión de atraques que asigna franjas horarias en función de la capacidad en tiempo real del destino, lo que evita que más de 8 000 pasajeros de cruceros lleguen a la isla al mismo tiempo.

- **Relación con el marco europeo:**
 - **Destino turístico inteligente (STD):** uso de la tecnología para equilibrar la economía turística con la sostenibilidad social y física.
- **Resiliencia para el estudiante:** Un recepcionista o guía puede consultar el calendario digital de cruceros y aconsejar al cliente que evite las zonas críticas durante las horas punta de desembarque, garantizando así la satisfacción y la seguridad del turista.

B. **Caso 2:** Astipalea – La primera isla «inteligente y sostenible»

- **El problema:** La dependencia de los combustibles fósiles para la energía y el transporte en las islas pequeñas conlleva altos costes, contaminación y vulnerabilidad ante problemas de suministro.
- **La iniciativa «inteligente»:** Un proyecto piloto integral que sustituye el transporte tradicional por vehículos eléctricos compartidos gestionados a través de una aplicación («AstyMove») y una red eléctrica inteligente alimentada con energía renovable.
- **Relación con el marco europeo:**
 - **Pacto Verde de la UE:** Reducción drástica de las emisiones en zonas aisladas y fomento de la movilidad limpia.
- **Resiliencia para los estudiantes:** Los estudiantes aprenden cómo la transición energética digital hace que un destino sea más autosuficiente y resiliente ante las crisis de los precios de la energía o las interrupciones en el suministro externo.



C. **Caso 3:** La aplicación «Extrema» para las olas de calor en Atenas

- **El problema:** Las temperaturas que superan los 40 °C en verano suponen un riesgo para la vida de los turistas que visitan la Acrópolis y otros yacimientos arqueológicos expuestos.
- **La acción «inteligente»:** una aplicación que utiliza datos satelitales en tiempo real para proporcionar información sobre el riesgo de calor calle por calle y sugiere «rutas frescas» y puntos de agua cercanos.
- **Relación con el marco europeo:**
 - **ODS 3 (Salud y bienestar) y 13 (Acción por el clima):** uso de la tecnología para proteger la vida humana frente a fenómenos meteorológicos extremos.
- **Resiliencia para el estudiante:** El experto en resiliencia utiliza estas herramientas digitales para recomendar horarios de visita seguros para sus grupos, activando los protocolos sanitarios antes de que se produzca una emergencia médica.

D. **Caso 4:** Digitalización del patrimonio y gestión de colas (entrada electrónica)

- **El problema:** El exceso de afluencia en los 25 principales yacimientos arqueológicos de Grecia provoca colas de varias horas bajo el sol, lo que afecta a la salud de los visitantes y a la eficiencia del personal.
 - **La acción «inteligente»:** Un sistema nacional de entradas electrónicas con franjas horarias obligatorias que distribuye la demanda a lo largo del día.
- **Relación con el marco europeo:**
 - **Estrategia Digital de la UE:** Digitalización de los servicios públicos para mejorar la eficiencia y la seguridad de los ciudadanos.
- **Resiliencia para los estudiantes:** Los estudiantes comprenden que la digitalización del acceso no es solo una cuestión de comodidad, sino una medida de resiliencia operativa que permite la evacuación ordenada de un yacimiento en caso de emergencia.

E. **Caso 5:** Comunicación digital de emergencias en Rodas (2023)

- **El problema:** Los incendios forestales incontrolados requieren la evacuación masiva y rápida de miles de turistas de diferentes nacionalidades.
- **La acción «inteligente»:** uso extensivo de las redes sociales, los canales digitales oficiales y los sistemas de alerta móvil para coordinar las repatriaciones y los traslados en tiempo real.
- **Relación con el marco europeo:**
 - **Sistemas de alerta temprana (EWS):** integración de señales de peligro en la comunicación directa con los turistas.
- **Resiliencia para el estudiante:** El estudiante practica la gestión de la información bajo presión, utilizando canales digitales para tranquilizar a los clientes y ofrecer soluciones logísticas rápidas, protegiendo la reputación del destino incluso durante una crisis.

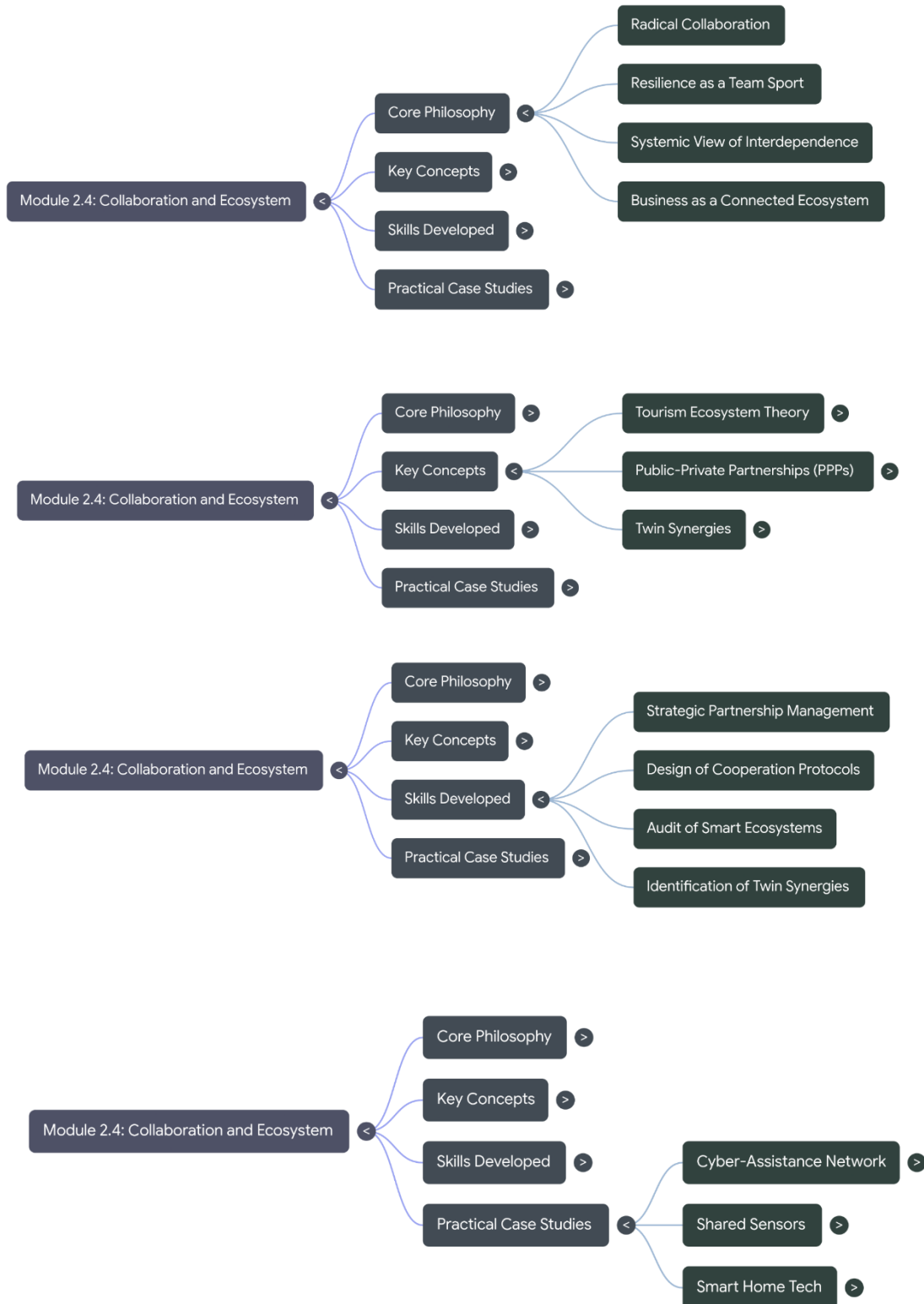
2.2.4 Colaboración y ecosistema (2 horas)

Este último módulo de **la subunidad 2** es donde encajan todas las piezas del rompecabezas. Aquí, los estudiantes aprenden que la resiliencia no es un «esfuerzo individual», sino un **deporte de equipo**. A lo largo de estas 4 horas, transformaremos la idea de la empresa como una isla en la visión de un **ecosistema conectado**, donde la colaboración con los vecinos, los ayuntamientos y las empresas tecnológicas es lo que realmente salva a la empresa cuando se produce una crisis.

El eje central de este módulo es **la colaboración radical**. En el sector turístico, si el destino sufre un contratiempo (una inundación, un ciberataque masivo a la red de la ciudad o una crisis de reputación), tu hotel o agencia se verá afectado, incluso si tus sistemas internos funcionan a la perfección. Por lo tanto, el profesional resiliente debe ser capaz de forjar alianzas estratégicas antes de que se produzca una emergencia.

Analizaremos cómo hablar el mismo idioma que los proveedores de tecnología y cómo participar en los foros de toma de decisiones de las autoridades públicas. Además, profundizaremos en la «magia» de **las sinergias**: cómo una única inversión (por ejemplo, una cerradura inteligente) puede ahorrar energía (sostenibilidad), facilitar el registro de entrada (digitalización) y proporcionar datos sobre quién entra y sale en caso de emergencia (seguridad). El objetivo es que los alumnos comprendan que colaborar y buscar sinergias no es un gasto, sino la forma más inteligente de invertir en el futuro de la empresa.

Esquema de la unidad



1. Teoría (1 hora)

I. La teoría del ecosistema turístico

- **Concepto:** La resiliencia organizativa depende de la resiliencia de la comunidad y del destino.
- **Aplicación:** Una empresa turística debe identificar a sus *partes interesadas*: desde la policía local hasta el proveedor de Wi-Fi y las asociaciones de vecinos.
- **Resiliencia:** si todos actúan de forma coordinada, la recuperación tras una crisis es mucho más rápida.

II. Alianzas público-privadas (APP)

- **Concepto:** Cooperación entre la administración pública y las empresas para alcanzar objetivos comunes.
- **Aplicación:** Participar en los planes de emergencia del ayuntamiento o en proyectos de «ciudad inteligente».
- **Resiliencia:** Proporciona acceso a sistemas oficiales de alerta temprana (EWS) que la empresa no podría permitirse por sí sola.

III. Inversiones con doble finalidad (sinergias dobles)

- **Concepto:** Buscar soluciones tecnológicas que aborden dos o más problemas al mismo tiempo.
- **Aplicación:** Implantación de sistemas domésticos inteligentes (IoT).
- **Sinergia:** Una cámara con inteligencia artificial puede contar turistas para evitar el exceso de aforo (seguridad/resiliencia) y, al mismo tiempo, apagar las luces en las zonas vacías (sostenibilidad/ahorro energético).

2. Competencias desarrolladas en esta unidad

Al finalizar este módulo y las actividades prácticas de la unidad, el estudiante habrá adquirido las siguientes competencias:

- **Gestión estratégica de alianzas:** Capacidad para colaborar activamente con las autoridades públicas (ayuntamientos, protección civil) y los proveedores de tecnología, participando en foros de toma de decisiones y planes de emergencia.
- **Identificación de «sinergias gemelas»:** capacidad para identificar oportunidades de inversión en las que una solución digital mejore simultáneamente la sostenibilidad y la seguridad operativa (p. ej., domótica e Internet de las cosas).
- **Diseño de protocolos de cooperación:** Competencia para redactar acuerdos de responsabilidad compartida que definan tareas específicas para la empresa, el proveedor técnico y la autoridad pública durante una crisis.
- **Análisis crítico de los ecosistemas inteligentes:** Capacidad para auditar soluciones tecnológicas en destinos turísticos inteligentes (STD), evaluando su impacto en la resiliencia climática y la vulnerabilidad digital.
- **Visión sistémica de la resiliencia:** Comprensión de la interdependencia entre la resiliencia organizativa y la comunitaria, identificando a *las partes interesadas* clave del entorno.

3. Casos concretos (1 hora)

I. Caso 1: La red de hoteles y la «ciberasistencia» local

- **Escenario:** Un grupo de pequeños hoteles rurales de un pueblo decide que ninguno de ellos puede permitirse contratar a un experto en ciberseguridad.
- **La acción:** Colaboran con una asociación tecnológica local para crear un «protocolo de ayuda mutua». Si uno detecta un correo electrónico sospechoso, se avisa automáticamente a los demás y a la policía.

Demuestra la capacidad de cooperar con compañeros y otras *partes interesadas* en situaciones de alto riesgo.

II. Caso 2: El ayuntamiento y los «sensores compartidos»

- **Situación:** Una oficina de turismo y los restaurantes de una plaza colaboran para instalar sensores de calidad del aire y de ruido.

- **La acción:** El ayuntamiento proporciona la red wifi y los negocios ceden el espacio para los sensores.
- **La sinergia:** Los datos ayudan al ayuntamiento a gestionar el ruido (relaciones de vecindad) y permiten al restaurante demostrar a sus clientes que su terraza es un espacio saludable y seguro.

Esto nos permite identificar sinergias entre la digitalización y la sostenibilidad.

III. **Caso 3:** Tecnología doméstica inteligente que protege y ahorra (caso de sinergia pura)

- **Situación:** Un albergue moderno instala cerraduras electrónicas que funcionan a través del móvil del huésped.
- **La acción:** El sistema está conectado al aire acondicionado de las habitaciones.
- **Resultado:** Cuando el huésped se marcha (el sensor detecta que no hay nadie presente), el aire acondicionado se apaga (ahorro/sostenibilidad). Además, el sistema registra que la habitación está vacía, lo que facilita el trabajo de los servicios de emergencia en caso de incendio (resiliencia/seguridad).

Evaluación de soluciones inteligentes para mejorar la resiliencia.

2.2.5 Actividades en grupo y resultados (7 horas)

Para estas 16 horas, se proponen tres actividades:

Actividad 1: Estudio de caso de un «destino inteligente» (3 horas)

- **Tarea:** El estudiante (o grupo) debe elegir uno de los siguientes destinos turísticos inteligentes reconocidos por la Comisión Europea:
 - Málaga (España): líder en gestión de la movilidad y eficiencia energética.
 - Gotemburgo (Suecia): un referente en sostenibilidad medioambiental y accesibilidad digital.
 - Valencia (España): pionera en la medición de la huella de carbono y la huella hídrica mediante datos en tiempo real.

- **Entrega: Informe de diagnóstico inteligente.** El estudiante debe **identificar una solución tecnológica utilizada por el destino** y explicar cómo mejora la resiliencia ante el cambio climático.

El informe debe seguir este marco técnico para garantizar que se abarcan todas las competencias del perfil TREADS:

1. Auditoría de «sinergias gemelas» (verde y digital)
 - **Identificación de los ODS:** ¿A qué Objetivos de Desarrollo Sostenible se dirige el destino con su estrategia tecnológica?
 - **Sinergia identificada:** Describir un ejemplo en el que la tecnología digital mejore directamente un factor medioambiental (p. ej., sensores de riego que ahorran agua).
2. Evaluación de las tecnologías implementadas

El estudiante debe analizar críticamente el uso de:

- **Sensores del IoT:** ¿Cómo controlan el consumo de energía y agua o los niveles de ocupación en el destino?
 - **Sistemas de IA:** ¿Cómo se utiliza la inteligencia artificial para predecir la demanda turística o responder a las crisis climáticas (por ejemplo, alertas de calor)?
3. Análisis de vulnerabilidad digital

En consonancia con la visión de un «experto consciente de los riesgos digitales», el estudiante debe responder a lo siguiente:

- **Amenaza detectada:** ¿Qué ocurriría si la infraestructura inteligente analizada (sensores, red de datos) sufriera un ciberataque?
 - **Medida de ciberresiliencia:** Proponer una medida de seguridad básica para proteger estos activos tecnológicos (p. ej., protocolos de acceso o cifrado de datos).
4. Matriz de diagnóstico (herramienta de trabajo)

Para facilitar el análisis, el alumno completará la siguiente tabla en su informe:

Unidad formativa I: Resiliencia en el Turismo

Componente inteligente	Tecnología (IoT/IA)	Riesgo climático mitigado	Vulnerabilidad digital asociada
Gestión del agua	Sensores de caudal en redes urbanas	Escasez de agua / Sequía	Manipulación de datos de consumo
Gestión energética	Redes inteligentes y automatización hotelera	Olas de calor / Picos de consumo	Acceso no autorizado a los sistemas de control
Flujos turísticos	IA para la previsión de ocupación	Hacinamiento / Inestabilidad	Robo de datos sobre el comportamiento de los clientes

5. Conclusiones y recomendaciones

El estudiante debe concluir el informe con una **propuesta de mejora**. ¿Qué tecnología adicional o medida de seguridad digital recomendarías al destino para que sea más resiliente en el futuro?

Metodología de evaluación de la Actividad 1

Para superar esta actividad, el formador evaluará la capacidad del alumno para:

1. **Identificar y clasificar correctamente los riesgos** en el caso práctico elegido.
2. **Evaluar soluciones inteligentes** que mejoren la resiliencia.
3. **Colaborar en la elaboración del informe escrito**, demostrando habilidades para la resolución de problemas.

Actividad 2: Auditoría de sinergias (2 horas)

- **Tarea:** Desarrollar un enfoque crítico para identificar soluciones tecnológicas que reduzcan el impacto medioambiental y, al mismo tiempo, evaluar cómo proteger digitalmente esta nueva infraestructura para garantizar la resiliencia empresarial.

Los alumnos, preferiblemente **trabajando en grupos**, deben **elegir una empresa relacionada con el turismo** (un hotel, una agencia de viajes o una empresa de transporte) y **analizar sus procesos actuales** con el fin de **proponer tres medidas de aplicación de la «Transición Doble»**.

Paso 1: Identificar áreas de mejora

El grupo debe elegir tres áreas críticas de consumo o impacto:

- Gestión del agua y de los residuos.
- Consumo energético y aire acondicionado.
- Gestión de residuos y plásticos de un solo uso.
- Movilidad y transporte de clientes.

Paso 2: Propuesta tecnológica (sinergia digital)

Para cada área, debes proponer una tecnología específica (IoT, IA o Big Data) que optimice ese recurso, basándote en los principios de la **economía circular** y los **ODS**.

Paso 3: Análisis de seguridad (resiliencia)

En consonancia con el perfil de un «experto en riesgos digitales», debes identificar qué ocurriría si esa tecnología fuera objeto de un ataque y cómo protegerla.

– Entrega:

1. Plan de sinergia.

El resultado final será un **Plan de Sinergia** (documento de 2 a 3 páginas) que incluya:

1. **Una breve descripción de la empresa elegida.**
2. **La Matriz de Sinergias** completada.

Área de impacto	Solución digital propuesta	Beneficio medioambiental (ODS)	Riesgo digital (ciberseguridad)	Medida de protección
Por ejemplo: Energía	<i>Termostatos inteligentes con sensores de presencia (IoT)</i>	<i>Reducción de las emisiones de CO₂ (ODS 13) y ahorro de costes.</i>	<i>Acceso remoto no autorizado para manipular la temperatura.</i>	<i>Cifrado de las comunicaciones y segmentación de la red Wi-Fi.</i>
Punto 1				
Punto 2				
Punto 3				

Tabla2 : Ejemplo de una matriz de sinergias

3. **Fundamento estratégico:** Breve explicación de cómo estas medidas alinean a la empresa con el Pacto Verde de la UE y la Estrategia Digital de la UE.
4. **Conclusión sobre la resiliencia:** cómo la empresa está ahora mejor preparada para hacer frente a crisis climáticas y digitales simultáneas.

Metodología de evaluación de la Actividad 2

El formador evaluará el resultado final basándose en:

- **Capacidad de identificación:** ¿Son realistas y aplicables las sinergias propuestas?
- **Concienciación sobre los riesgos:** ¿Se ha identificado correctamente la vulnerabilidad digital asociada a la nueva tecnología?
- **Pensamiento sistémico:** ¿Se han integrado de forma coherente los principios de sostenibilidad y digitalización?
- **Trabajo en equipo:** en el caso del trabajo en grupo, la calidad de la presentación y la resolución de problemas durante el taller.

Actividad 3: El Círculo de Resiliencia (2 horas)

- **Objetivo:** Desarrollar la capacidad de **colaborar con las autoridades públicas y los proveedores de tecnología** para implementar medidas de resiliencia basadas en la digitalización y la sostenibilidad.

Fase 1: Mapeo de partes interesadas y gobernanza (60 minutos)

En esta fase, el alumno debe **identificar** con quién debe **cooperar** para garantizar que su **plan de resiliencia sea eficaz**.

- **Tarea 1.1:** Selecciona una «parte interesada pública» (por ejemplo, una oficina de turismo o Protección Civil) y define qué información del sistema de alerta temprana (EWS) puede proporcionar.
- **Tarea 1.2:** Selecciona un «proveedor de tecnología» (por ejemplo, una empresa de IoT o de apoyo a la ciberseguridad) y define qué herramientas inteligentes proporcionará para apoyar la resiliencia.
- **Tarea 1.3:** Definir un canal de comunicación mutuo para cooperar con estas partes interesadas durante una situación de crisis.

Fase 2: Diseño de la sinergia «doble» (60 minutos)

El alumno debe **proponer una inversión** que cumpla los objetivos de la «transición doble» (verde y digital).

- **Tarea 2.1:** Identificar una vulnerabilidad climática o medioambiental (por ejemplo, escasez de agua u olas de calor).
- **Tarea 2.2:** Proponer una solución digital (por ejemplo, sensores de caudal de agua basados en el IoT o sistemas domésticos inteligentes para el control de la climatización).
- **Tarea 2.3:** Evaluar cómo esta solución inteligente mejora simultáneamente la resiliencia y la sostenibilidad (sinergia).
- **Tarea 2.4:** Identificar el riesgo digital asociado a esta nueva tecnología y proponer una medida básica de ciberseguridad.

Fase 3: Protocolo de responsabilidad compartida (60 minutos)

En esta fase, los alumnos practican la autonomía y la responsabilidad a la hora de llevar a cabo tareas de resiliencia. El alumno redactará un breve «Acuerdo de Cooperación» que incluya:

1. **Responsabilidad empresarial:** Tareas rutinarias de resiliencia que deberá llevar a cabo el alumno de acuerdo con los procedimientos establecidos (p. ej., supervisar el panel de control de consumo).
2. **Responsabilidad del proveedor:** Asistencia técnica en caso de fallos en los sistemas inteligentes.
3. **Responsabilidad de las autoridades:** Suministro de datos climáticos en tiempo real o alertas de seguridad.

Ejemplo de entrega: Formulario de acuerdo de cooperación

Nombre del estudiante: _____

Nombre de la organización: _____

Fecha: XX/XX/202X

1. Identificación del ecosistema

Identifica a tus socios estratégicos para la implementación de medidas de resiliencia.

Parte interesada	Organización / Empresa	Función en materia de resiliencia
Autoridad pública	(p. ej., Oficina de Turismo local)	Proporcionar alertas tempranas y marcos jurídicos.
Proveedor de tecnología	(p. ej., empresa de ciberseguridad/IoT)	Implementar y garantizar la seguridad de soluciones inteligentes.
Socio comunitario	(p. ej., asociación hotelera)	Cooperación y apoyo mutuo durante la crisis.

2. Definición de la sinergia «Twin» (transición doble)

Describir la solución que integra la sostenibilidad y la digitalización para mejorar la resiliencia.

- **Objetivo de Desarrollo Sostenible (ODS):** (p. ej., ODS 6: gestión eficiente del agua).
- **Solución digital inteligente:** (p. ej., sensores IoT para la detección de fugas en tiempo real).
- **Justificación de la sinergia:** (Explica cómo la tecnología respalda el objetivo ecológico y cómo protege a la empresa de los riesgos medioambientales).

3. Protocolo sobre responsabilidades y autonomía

Define las tareas específicas de cada parte para garantizar la continuidad del negocio.

- **Responsabilidad del estudiante (autonomía):** Tareas rutinarias, como supervisar los indicadores de alerta temprana y cumplir los procedimientos de resiliencia.
- **Responsabilidad del proveedor tecnológico:** Apoyo en la recuperación de datos tras una crisis y mantenimiento de la ciberseguridad dentro de la infraestructura.
- **Responsabilidad de la autoridad:** Emitir señales de escalamiento de crisis y coordinar la respuesta a nivel local.

4. Gestión de crisis y comunicación

Establecer cómo se llevará a cabo la cooperación en situaciones de presión.

- **Canal de comunicación:** (por ejemplo, un grupo de mensajería instantánea segura o la plataforma Smart Destination).
- **Señales de alerta temprana (EWS):** enumerar los indicadores que activarán este acuerdo (p. ej., informe de sequía extrema o alerta de un ciberataque masivo).
- **Prioridad de actuación:** Definición de qué servicios se protegerán en primer lugar en caso de crisis.

Metodología de evaluación de la actividad 3

El formador evaluará el rendimiento del alumno basándose en los siguientes criterios del plan TREADS:

1. **Capacidad de colaboración:** ¿Has identificado y clasificado correctamente a las partes interesadas y sus funciones?
2. **Resolución de problemas:** ¿Es lógica la sinergia propuesta y aplica los principios de sostenibilidad y digitalización?
3. **Autonomía:** ¿Has demostrado la capacidad de tomar decisiones y proponer acciones bajo una situación de presión simulada?

Además, el rendimiento de los alumnos se evaluará mediante cuestionarios.

Cuestionario:

1. ¿Qué tecnología es clave para controlar el consumo de agua y energía en un hotel resiliente?
 - A. Las redes sociales.
 - B. Sensores del IoT.
 - C. Hojas de cálculo manuales.
 - D. Publicidad programática.
2. La «doble transición» se refiere a la transición conjunta hacia:
 - A. El lujo y el bajo coste.
 - B. Lo rural y lo urbano.
 - C. Lo ecológico (sostenible) y lo digital.
 - D. Transporte aéreo y marítimo.
3. ¿Cuál es uno de los efectos del cambio climático en la estacionalidad del turismo?
 - A. Una reducción de los costes de marketing.
 - B. Un cambio en los flujos turísticos debido a olas de calor extremas.
 - C. Una mayor ciberseguridad.

D. Un aumento automático de la resiliencia de la comunidad.

2.3 Planificación de la resiliencia en el turismo

Al finalizar esta subunidad, los alumnos serán capaces de contribuir a un plan básico de respuesta ante crisis, participar en los procesos de toma de decisiones en situaciones de crisis y priorizar acciones bajo presión.

- I. Ciclo de vida de una crisis: prevención, preparación, respuesta, recuperación y aprendizaje
- II. Enfoque en:
 - las estrategias de recuperación tras una crisis para las empresas turísticas
 - recuperación de la reputación y la confianza (opiniones en línea, relaciones con los medios de comunicación, comunicación con los clientes)
 - análisis posteriores a la intervención y mejora continua
- III. Gestión de crisis en tres ámbitos: salud, clima y ámbito digital.

Actividad práctica sugerida:

Juego de roles: simulación de un comité de gestión que responde a una crisis en una empresa turística, como un hotel.

Mientras que las unidades anteriores trataban sobre la evaluación de la situación (Unidad 1) y la dotación de tecnología sostenible (Unidad 2), **la Subunidad 3** es la simulación de la respuesta. Aquí es donde el alumno deja de ser un observador y se convierte en un gestor activo que debe tomar decisiones difíciles mientras el tiempo corre.

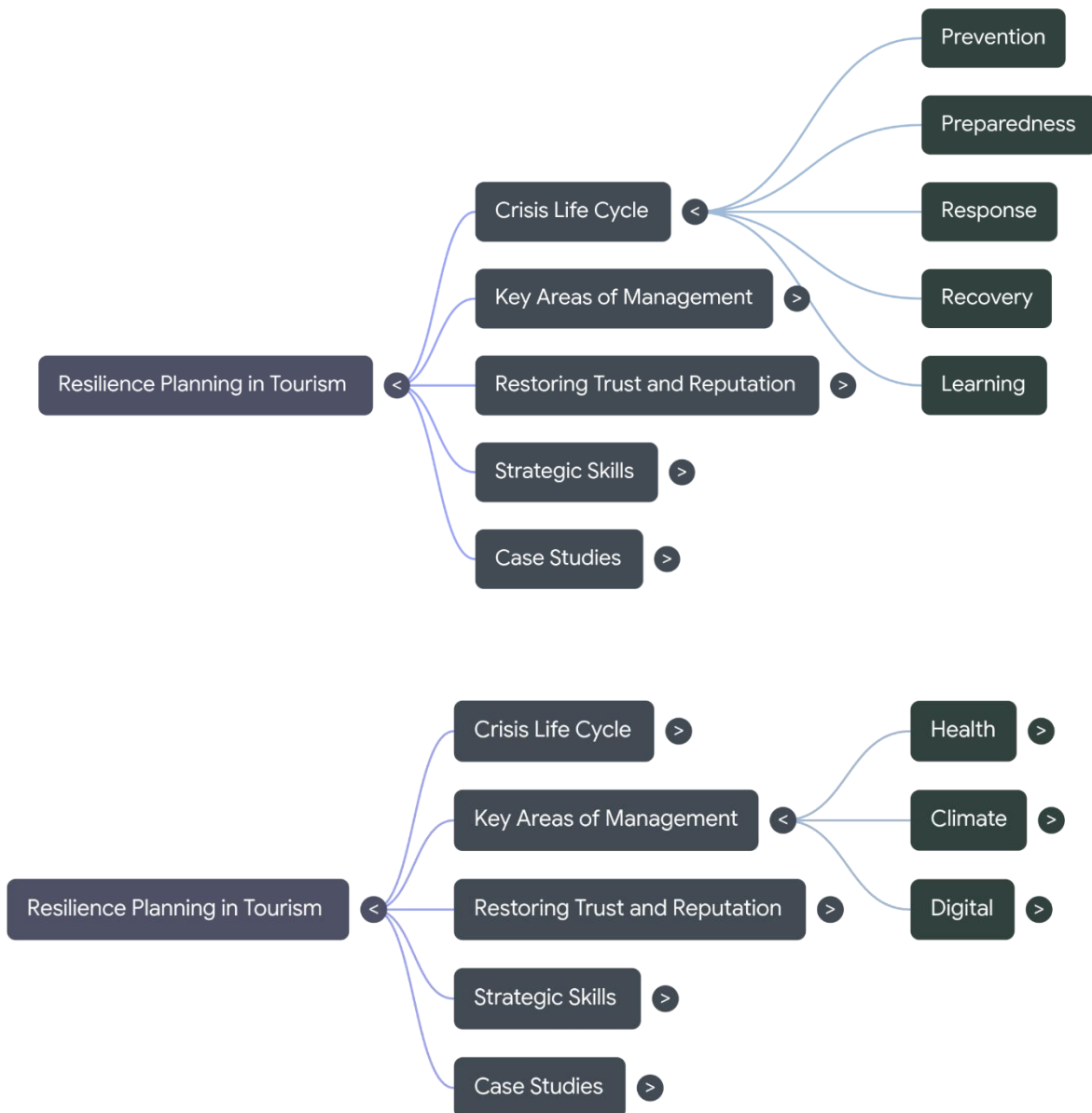
Esta subunidad no trata de evitar que las cosas salgan mal, sino de qué hacer cuando, inevitablemente, algo sale mal. Se centra principalmente **en la planificación de la respuesta** y, lo más importante, **en restablecer la confianza**. En un entorno en el que las noticias se propagan como la pólvora en las redes sociales y una sola reseña negativa puede arruinar una temporada, la resiliencia se mide por la rapidez y la calidad de la respuesta.

Los alumnos aprenderán a gestionar el **ciclo de vida de una crisis** —desde la preparación discreta hasta el aprendizaje posterior al incidente— especializándose

Unidad formativa I: Resiliencia en el Turismo

en tres áreas críticas: salud, clima y ámbito digital. No buscamos teóricos, sino profesionales capaces de formar parte de un comité de crisis, mantener la cabeza fría bajo presión y priorizar las acciones que protejan tanto a las personas como a la reputación de la marca.

Resumen de la unidad



Unidad formativa I: Resiliencia en el Turismo



1. Marco teórico. El ciclo de vida de una crisis

La teoría que se aborda en esta subunidad es la siguiente:

1. El ciclo de vida de una crisis y la preparación (4 horas)

- **Sesión teórica (1,5 horas):** Introducción a las cinco fases del ciclo de vida de una crisis: prevención, preparación, respuesta, recuperación y aprendizaje.
- **Taller de auditoría (1,5 horas):** Identificación de protocolos específicos de prevención y preparación para cuestiones sanitarias, climáticas y digitales.
- **Sesión de liderazgo (1 hora):** El papel de la adaptabilidad y el factor humano en la toma de decisiones bajo presión.

2. Respuesta operativa en las tres áreas clave (1 hora)

- **Sesión teórica (1 hora):** Priorización de acciones en el «punto cero» de la crisis. Análisis de las áreas prioritarias de seguridad personal (salud), protección de infraestructuras (clima) y aislamiento de sistemas (digital).

3. Restablecimiento de la confianza y la reputación (1,5 horas)

- **Sesión teórica (1,5 horas):** Estrategias de recuperación tras la crisis para empresas turísticas. Énfasis en la gestión de las reseñas en línea, las relaciones con los medios de comunicación y la comunicación directa con los clientes.

2. Competencias adquiridas

Al finalizar estas 16 horas, el alumno habrá desarrollado las siguientes competencias fundamentales:

- **Contribución técnica:** Capacidad para aportar contenidos específicos a un plan básico de respuesta ante crisis.
- **Toma de decisiones:** Participación activa en los procesos de toma de decisiones durante situaciones críticas, demostrando liderazgo y capacidad de adaptación.

- **Priorización estratégica:** Capacidad para priorizar y ejecutar acciones bajo una gran presión, distinguiendo entre lo que es urgente y lo que es vital.
- **Gestión de la reputación:** Competencia en el diseño de estrategias para restablecer la confianza y gestionar la comunicación con los clientes y los medios de comunicación.
- **Análisis crítico:** Capacidad para llevar a cabo análisis posteriores a la acción con el fin de fomentar la mejora continua.
- **Prevención:** Medidas para evitar que se produzcan riesgos (mantenimiento, ciberhigiene).
- **Preparación (proactividad):** Creación de protocolos, asignación de funciones y realización de simulacros.
- **Actuación bajo presión**
- **Recuperación:** estrategias para volver a la normalidad operativa y financiera.
- **Aprendizaje (verdadera resiliencia):** El «análisis posterior a la acción». Analizar qué salió mal y actualizar el plan para garantizar que no vuelva a ocurrir.

3. Casos prácticos

I. Sector digital: Meliá Hotels International (ciberataque de 2021) (1 hora)

Este es el caso práctico por excelencia para analizar **la respuesta y la recuperación** ante una amenaza digital.

- **La crisis:** La cadena hotelera sufrió un ataque *de ransomware* que bloqueó sus sistemas operativos en plena fase de recuperación del turismo.
- **Aplicación del ciclo (respuesta):** Meliá decidió **no pagar el rescate**. En su lugar, activó un comité de crisis que dio prioridad a la «continuidad del negocio» mediante procesos manuales, al tiempo que se restauraban los sistemas a partir de copias de seguridad.

- **Restablecimiento de la confianza:** La empresa mantuvo una comunicación transparente con los clientes y el mercado, lo cual es una piedra angular para la **recuperación de la reputación**.
- **Lecciones aprendidas:** Reforzaron su infraestructura bajo el modelo «Zero Trust», implementando mejoras continuas tras el análisis del incidente.

II. Sección sobre el clima: El Grupo TUI y los incendios en Rodas (2023) (1 hora)

Un ejemplo perfecto de cómo **priorizar las acciones bajo presión** ante un desastre natural.

- **La crisis:** Miles de turistas tuvieron que ser evacuados debido a unos incendios forestales incontrolables en Grecia.
- **Aplicación del ciclo (respuesta):** TUI activó un equipo de respuesta rápida (Equipo de Gestión de Crisis) para coordinar los vuelos de repatriación y el realojamiento de los clientes, dando prioridad a **la seguridad de las personas**.
- **Comunicación de crisis:** Utilizaron sus canales digitales y redes sociales para ofrecer información actualizada minuto a minuto, gestionando **las opiniones en línea y las relaciones con los medios de comunicación** para evitar el pánico.
- **Estrategia de recuperación:** Una vez superado el peligro, lanzaron campañas para demostrar que el destino volvía a ser seguro, con el fin de **restablecer la confianza** del mercado.

III. Sector sanitario: Marriott International (Consejo Global de Higiene) (1 hora)

Este caso ilustra la fase **de prevención y preparación** a escala mundial.

- **La crisis:** La pandemia de COVID-19 alteró radicalmente los estándares sanitarios en el turismo.
- **Aplicación del ciclo (preparación):** Marriott no se limitó a reaccionar, sino que creó un «Consejo Global de Higiene» para diseñar nuevos protocolos de higiene antes de la reapertura total.

- **Reputación y confianza:** Implementaron sellos de seguridad visibles y tecnologías sin contacto para que los clientes se sintieran seguros, lo cual es clave para **restablecer la confianza de los consumidores**.
- **Lección aprendida:** Estas normas se han convertido en tareas rutinarias de resiliencia que el personal lleva a cabo de forma autónoma.

4. Dinámica de trabajo y resultados esperados

I. Aplicación práctica: Juego de roles «El Comité de Crisis. El laboratorio poscrisis» (6,5 horas)

Esta actividad transporta al alumno al día siguiente de la tormenta. El objetivo es que los alumnos analicen un fallo real, gestionen la reputación dañada y diseñen mejoras para que la organización sea más resiliente en el futuro.

◦ Preparación y diagnóstico (fase de análisis)

La clase se divide en grupos de 3 o 4 personas. A cada grupo se le entrega un «**expediente de crisis real**» (basado en los casos de salud, clima o digitales tratados anteriormente).

- **Tarea:** Identificar en qué punto del ciclo de vida falló la empresa (¿fue una prevención deficiente? ¿Falta de preparación? ¿Una respuesta inadecuada?).
- **Resultado:** un diagrama del ciclo de vida de esa crisis concreta, en el que se destaquen los «puntos de ruptura».

◦ El Gabinete de Reputación (Gestión de la confianza)

Los alumnos deben abordar las consecuencias públicas del incidente.

- **Actividad:** Se les entregan cinco «comentarios negativos críticos» de clientes ficticios en plataformas como TripAdvisor o Google Reviews tras el incidente.
- **Tarea:** Redactar las respuestas oficiales de la empresa y diseñar un comunicado de prensa que dé prioridad a la transparencia y al restablecimiento de la confianza.

- **El taller de mejora continua (análisis posterior a la acción)**

Siguiendo los principios de la mejora continua, el grupo debe actuar como consultores de resiliencia.

- **Tarea:** Redactar un **informe de análisis posterior a la acción (AAR)**. Este documento debe incluir:
 - Tres nuevas medidas preventivas para evitar que se repita la situación.
- Un ajuste específico al plan básico de respuesta de la empresa.
- Estrategias de recuperación tras la crisis para garantizar la estabilidad financiera y operativa.

- **Base de datos de revisiones críticas para el ejercicio**

Para llevar a cabo la actividad, se proporcionará a los alumnos un conjunto de evaluaciones con las que trabajar:

- **Crisis sanitaria (intoxicación alimentaria/brote relacionado con la higiene)**

Opinión 1 (TripAdvisor – 1 estrella):

«¡Evita este hotel! Mi familia y yo pasamos las vacaciones en el hospital por culpa del bufé. Ningún miembro del personal nos ayudó ni nos dio ninguna explicación. Lo único que les importaba era que no hiciéramos ruido. ¡Una gestión vergonzosa!»

- **Reto para el estudiante:** ¿Cómo se puede pedir disculpas sin admitir responsabilidad legal inmediata antes de que concluya la investigación, al tiempo que se muestra empatía humana?
- **Crisis climática (fallo en la evacuación/información)**

Opinión 2 (Google Maps – 2 estrellas):

«Nos evacuaron por las inundaciones, pero fue un caos total. El personal no sabía adónde enviarnos y nos dejó bajo la lluvia durante dos horas sin mantas ni agua. Entiendo que el tiempo no es culpa suya, pero la falta de un plan sí que lo es. No volveremos».

- **Reto para el estudiante:** Argumentar que la seguridad era la prioridad, pero reconocer los fallos logísticos y explicar las mejoras para el futuro.
- **Crisis digital (ciberataque/filtración de datos)**

Comentario 3 (Booking.com – 1 estrella):

«Me acaban de decir que mis datos bancarios se han filtrado debido a un “fallo informático” en vuestra página web de reservas. Es inaceptable que una empresa de este calibre tenga una seguridad tan deficiente. Ahora tengo que bloquear todas mis tarjetas. ¡Exijo una indemnización!».

- **Reto para el estudiante:** Restablecer la confianza en el aspecto técnico. ¿Qué medidas de ciberseguridad se han adoptado para garantizar que esto no vuelva a suceder?
- **Guía de respuestas: Las «reglas de oro» para los estudiantes**

Para que los estudiantes respondan de forma profesional, deben seguir estos cuatro pasos en cada respuesta:

- **Validación:** Reconocer los sentimientos del cliente (p. ej., «Lamentamos profundamente su frustración...»).
- **Acción inmediata:** Explicar qué se hizo en su momento para contener los daños.
- **Compromiso de mejora (aprendizaje):** Mencionar el cambio específico (p. ej., «Hemos implementado nuevos protocolos para...»).
- **Canal privado:** Trasladar la conversación fuera del foro público (p. ej., «Póngase en contacto con nosotros en [correo electrónico] para que podamos resolver su problema personalmente»).
- **Actividad complementaria: Matriz de priorización**

La matriz de priorización es una herramienta técnica y estratégica fundamental dentro del programa TREADS, diseñada para permitir a los profesionales del turismo tomar decisiones eficaces en situaciones de gran presión. Su principal objetivo es ayudar a clasificar las tareas y respuestas

necesarias durante una crisis, permitiendo distinguir claramente entre lo que es **urgente** y lo que es **vital** para la supervivencia de la organización.

En el contexto de la gestión de crisis, la matriz actúa como un **filtro para la toma de decisiones**. No todas las amenazas o incidentes requieren la misma rapidez o el mismo tipo de respuesta. La matriz permite asignar **los recursos** (tiempo, personal, dinero) de forma lógica, basándose en un análisis de los posibles daños.

Los alumnos deben completar esta tabla antes de redactar sus respuestas:

Resumen	Nivel de riesgo (1-10)	Impacto en la marca	Acción prioritaria
Salud	10	Muy alto (Aspectos legales/Vidas humanas)	Investigación sanitaria y desinfección.
Clima	7	Medio (Operativo)	Revisión de los protocolos de evacuación.
Digital	9	Alto (Privacidad/Aspectos legales)	Auditoría del sistema y notificación a las autoridades.

Donde Riesgo (R) = Probabilidad (P) × Impacto (I)

◦ Conclusión del ejercicio

Al final de la clase, cada grupo leerá en voz alta su respuesta más difícil. El resto de la clase actuará como «público» y decidirá si la respuesta restaura su confianza en la empresa o si suena a «excusa corporativa».

5. Evaluación

El formador evaluará la capacidad de los alumnos para participar en procesos de toma de decisiones y su habilidad para elaborar planes de acción coherentes que integren los ámbitos de la salud, el clima y la tecnología digital basándose en los siguientes puntos:

1. Fase de diagnóstico y análisis

- **Precisión en la identificación del fallo:** la capacidad del grupo para señalar correctamente en qué etapa del ciclo de vida (prevención, preparación o respuesta) se produjo el principal error de la empresa.
- **Calidad técnica del diagrama:** claridad y coherencia del diagrama de «puntos de ruptura» que ilustra la escalada de la crisis concreta.

2. Gestión de la reputación y la confianza

- **Aplicación de las «reglas de oro»:** estricto cumplimiento de los cuatro pasos a seguir en las respuestas a las reseñas: validación del sentimiento, explicación de las medidas inmediatas, compromiso de mejora y derivación a un canal privado.
- **Equilibrio comunicativo:** capacidad para mostrar empatía humana y transparencia sin comprometer la responsabilidad legal de la empresa antes de que concluyan las investigaciones.
- **Eficacia del comunicado de prensa:** capacidad para elaborar un mensaje que restablezca la confianza del mercado y de los medios de comunicación tras el incidente.

3. Taller de mejora continua (informe AAR)

- **Pertinencia de las medidas preventivas:** viabilidad y pertinencia de las tres nuevas medidas propuestas para evitar que se repita el incidente.
- **Coherencia en el ajuste del plan:** Calidad técnica del cambio propuesto al plan básico de respuesta de la organización.
- **Visión de recuperación:** solidez de las estrategias propuestas para garantizar la estabilidad financiera y operativa tras la crisis.

4. Matriz de priorización

- **Criterios de clasificación:** Capacidad para distinguir correctamente entre acciones «urgentes» y acciones «vitales» para la supervivencia de la empresa en situaciones de presión.
- **Lógica en la asignación de recursos:** Coherencia en el uso de la matriz como filtro para la toma de decisiones basado en el análisis de los daños potenciales.

5. Competencias transversales

- **Toma de decisiones bajo presión:** Participación activa y liderazgo demostrado durante la simulación de crisis en tiempo real.
- **Integración de áreas críticas:** capacidad para elaborar planes de acción que unifiquen la gestión en los sectores de la salud, el clima y el ámbito digital.
- **Trabajo en equipo y defensa de posiciones:** Colaboración eficaz dentro del grupo y capacidad para defender los resultados y los mapas de riesgos ante el resto de la clase.

1. Teoría de los sistemas socioecológicos (SES)

- Adger, W. N. (2000). Resiliencia social y ecológica: ¿están relacionadas? *Progress in Human Geography*, 24(3), 347–364.
- Berkes, F., Folke, C. y Colding, J. (2002). *Navegando por los sistemas socioecológicos: desarrollar la resiliencia ante la complejidad y el cambio*. Cambridge University Press.
- Folke, C. (2016). Resiliencia (reedición). *Ecology and Society*, 21(4).
- García González, E. D., López Guevara, V. M. y López Pardo, G. (2022). Análisis de la resiliencia social en los sistemas socioecológicos: una propuesta interdisciplinaria para los destinos turísticos y su desarrollo sostenible. *Tourism Research*, (23), 48–72.
- Ostrom, E. (2009). Un marco general para analizar la sostenibilidad de los sistemas socioecológicos. *Science*, 325(5939), 419–422.

2. El ciclo de vida de las crisis (teoría de la gestión de crisis)

- Faulkner, B. (2001). Hacia un marco para la gestión de desastres en el turismo. *Tourism Management*, 22(2), 135–147.
- Glaesser, D. (2006). *Gestión de crisis en el sector turístico*. Elsevier Butterworth-Heinemann.
- Santana, G. (2004). Gestión de crisis y turismo. *Journal of Travel & Tourism Marketing*, 15(4), 299–321.

3. La teoría de las organizaciones de alta fiabilidad (HRO) y el factor humano

- Hall, C. M. (2010). Crisis y resiliencia en el turismo. *Tourism Recreation Research*, 35(3), 229–245.
- Sutcliffe, K. M. (2011). Organizaciones de alta fiabilidad (HRO). *Best Practice & Research Clinical Anaesthesiology*, 25(2), 133–144.
- Weick, K. E. y Sutcliffe, K. M. (2007). *Gestionar lo inesperado: rendimiento resiliente en una era de incertidumbre*. Jossey-Bass.

- Weick, K. E., Sutcliffe, K. M. y Obstfeld, D. (1999). Organizarse para una alta fiabilidad: procesos de atención plena colectiva. *Research in Organizational Behavior*, 21, 81–123.

4. Modelo de gestión de riesgos (matriz de probabilidad e impacto)

- Centro Internacional de Turismo Sostenible de la APEC. (2007). *Gestión de riesgos en el turismo: una guía de referencia para la gestión de crisis en el sector turístico*. APEC.
- Organización Internacional de Normalización. (2018). *Gestión de riesgos: directrices* (Norma ISO n.º 31000:2018).
- Ritchie, B. W. (2004). Caos, crisis y desastres: un enfoque estratégico de la gestión de crisis en el sector turístico. *Tourism Management*, 25(6), 669–683.

5. Adaptación al cambio climático y gestión del riesgo operativo

Estas fuentes sustentan la teoría de los sistemas socioecológicos y el análisis técnico de las amenazas relacionadas con el clima en destinos costeros y de montaña.

- Adger, W. N. (2000). Resiliencia social y ecológica: ¿están relacionadas? *Progress in Human Geography*, 24(3), 347–364.
- Agencia Europea de Medio Ambiente (AEMA). (s. f.). *El cambio climático como amenaza para el turismo*.
- García González, E. D., López Guevara, V. M. y López Pardo, G. (2022). Análisis de la resiliencia social en los sistemas socioecológicos. *Tourism Research*, (23), 48–72.
- IPCC. (2023). Sexto Informe de Evaluación (AR6). Resumen para responsables de políticas.

6. «Transición doble» (transición verde y digital)

Documento normativo de la Unión Europea que define el marco jurídico y estratégico para la transición doble durante la próxima década.

- Comisión Europea. (2019). *El Pacto Verde Europeo*. COM(2019) 640 final.
- Comisión Europea. (2020). *Configurar el futuro digital de Europa*.
- Comisión Europea. (2022). *Ruta de transición para el turismo*.

7. Economía circular y sostenibilidad en el turismo

Recursos para apoyar el «Modelo R» y la integración de los Objetivos de Desarrollo Sostenible en la gestión hotelera.

- Fundación Ellen MacArthur. (s. f.). *La economía circular en los viajes y el turismo*.
- Naciones Unidas. (2015). *Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*. Resolución 70/1.
- Organización Mundial del Turismo (OMT). (s. f.). *El turismo en la Agenda 2030*.

8. Tecnologías digitales para la eficiencia en el uso de los recursos

Fundamentos teóricos para la implementación del Internet de las cosas (IoT), la inteligencia artificial y la gobernanza de datos en destinos turísticos inteligentes.

- Comisión Europea. (2021). *Ley de Inteligencia Artificial (propuesta de reglamento)*.
- Gretzel, U., et al. (2015). Turismo inteligente: fundamentos y desarrollos. *Electronic Markets*, 25(3), 179-188.
- SEGITTUR. (2022). *Guía de destinos turísticos inteligentes*.

9. IoT (Internet de las cosas): los ojos de la empresa

Esta sección se basa en la capacidad de los objetos físicos interconectados para recopilar datos en tiempo real y eliminar los puntos ciegos operativos.

- **Atzori, L., Iera, A. y Morabito, G. (2010).** El Internet de las cosas: un estudio. *Computer Networks*, 54(15), 2787-2805. (Un trabajo fundamental para comprender la arquitectura de red que subyace a los sensores de flujo y de energía).
- **Gubbi, J., Buyya, R., Marusic, S. y Palaniswami, M. (2013).** Internet de las cosas (IoT): una visión, elementos arquitectónicos y orientaciones futuras. *Future Generation Computer Systems*, 29(7), 1645-1660. (Respalda la teoría de la infraestructura compartida en destinos inteligentes).
- **SEGITTUR. (2022).** *Guía de destinos turísticos inteligentes*. Ministerio de Industria, Comercio y Turismo. (Base técnica para el seguimiento de los niveles de ocupación y el mantenimiento predictivo).

10. IA y big data: el cerebro de la respuesta ante crisis

Recursos que explican cómo la inteligencia artificial procesa grandes volúmenes de datos para predecir la demanda y activar sistemas de alerta temprana (EWS).

- **Gretzel, U., Sigala, M., Xiang, Z. y Koo, C. (2015).** Turismo inteligente: fundamentos y avances. *Electronic Markets*, 25(3), 179-188. (Define la capacidad de «predecir y decidir» de los sistemas inteligentes).
- **Mayer-Schönberger, V. y Cukier, K. (2013).** *Big Data: una revolución que transformará nuestra forma de vivir, trabajar y pensar*. Eamon Dolan/Houghton Mifflin Harcourt. (Apoya el uso de modelos de previsión y la optimización de recursos críticos).
- **Zhang, Y., y Li, G. (2023).** «La inteligencia artificial en la gestión de crisis: una revisión sistemática y orientaciones para futuras investigaciones». *Journal of Management Analytics*. (Específicamente para algoritmos que responden a crisis climáticas o sanitarias).

11. Ética y responsabilidad en la IA

Fuentes centradas en el uso responsable de la IA de acuerdo con la normativa europea, la transparencia y el tratamiento ético de los datos.

- **Comisión Europea. (2021).** *Ley de Inteligencia Artificial (propuesta de reglamento)*. (Documento jurídico clave sobre la transparencia en el tratamiento de datos biométricos).
- **Floridi, L. y Cowls, J. (2022).** *Un marco unificado de cinco principios para la IA en la sociedad*. En *Ethics, Governance, and Policies in Artificial Intelligence*. Springer. (Teoría sobre la equidad y la ausencia de manipulación en los algoritmos predictivos).
- **Jobin, A., Ienca, M. y Vayena, E. (2019).** El panorama global de las directrices éticas sobre la IA. **Nature Machine Intelligence**, 1(9), 389-399. (Fundamentos para la implementación de una IA responsable en el sector servicios).

12. Espacios de datos turísticos

Teoría sobre el intercambio seguro de indicadores de riesgo e información sobre sostenibilidad sin comprometer la privacidad ni los secretos comerciales.

- **Comisión Europea. (2022).** *Una estrategia europea para los datos*. (Define el marco para los espacios de datos comunes con el fin de reforzar la resiliencia colectiva).
- **Asociación Internacional de Espacios de Datos (IDSA). (2021).** *Reglamento para los espacios de datos*. (Apoya los protocolos de seguridad para compartir alertas en tiempo real sobre saturación y consumo).

- **Foro Económico Mundial. (2021).** *Colaboración en materia de datos por el bien común: fomentar la confianza y la innovación en el turismo.* (Explica cómo las empresas colaboran con las autoridades a través del intercambio de datos).

13. Ciberseguridad en la doble transición: protección de la infraestructura verde

Bibliografía sobre la protección de sensores de agua, paneles inteligentes y sistemas automatizados de climatización frente a nuevos vectores de ataque.

- **Agencia de Ciberseguridad de la Unión Europea (ENISA). (2023).** *Ciberseguridad en el sector turístico.* (Centrado en la protección de infraestructuras críticas y sistemas BMS).
- **Directiva (UE) 2022/2555 (NIS2).** Medidas destinadas a garantizar un alto nivel común de ciberseguridad en toda la Unión. (Marco jurídico que exige a las cadenas hoteleras reforzar su seguridad digital).
- **Humayun, M., Jhanjhi, N. Z., Hamid, B. y Ahmed, G. (2020).** La logística y el transporte inteligentes emergentes como un sistema de sistemas: una perspectiva de resiliencia. *IEEE Access.* (Analiza la amenaza que plantean la interconectividad y la seguridad desde el diseño en los sistemas de IoT).

14. La Guía de Sostenibilidad (Pacto Verde y ODS)

Esta sección se centra en cómo los compromisos europeos para reducir la contaminación y aumentar el ahorro se traducen en resiliencia operativa.

- **Fletcher, R., et al. (2020).** *El turismo y los Objetivos de Desarrollo Sostenible.* Routledge. (Analiza la aplicación práctica de los 17 ODS en los modelos de negocio del turismo).
- **Hall, C. M. (2019).** La construcción del desarrollo turístico sostenible: la Agenda 2030 y los ODS. *Journal of Sustainable Tourism*, 27(7), 1044-1060. (Explica la relación entre la agenda global y la viabilidad económica del sector).
- **Pascual, J. M. y Arcos, M. J. (2023).** *El turismo y el Pacto Verde Europeo: hacia la neutralidad climática para 2050.* Editorial Universitaria. (Respalda la teoría de que el ahorro energético y la reducción del plástico son medidas de resiliencia).

15. El Escudo Digital (Estrategia Digital de la UE)

Recursos centrados en las normas destinadas a hacer de Internet un lugar seguro, protegiendo los datos y la reputación mediante herramientas digitales sólidas.

- **Directiva (UE) 2022/2555 (Directiva NIS2).** Medidas destinadas a garantizar un alto nivel común de ciberseguridad en toda la Unión. (Marco jurídico en el que se sustenta el «Escudo Digital» para la cadena de suministro del turismo).
- **Comisión Europea. (2020).** *Una estrategia europea en materia de datos.* COM (2020) 66 final. (Define la soberanía digital y el uso de herramientas que «no fallan» a la hora de proteger la reputación corporativa).
- **Floridi, L. (2021).** *La ética de la información.* Oxford University Press. (Proporciona la base ética para el tratamiento seguro de los datos de los clientes, esencial para prevenir el phishing y la pérdida de confianza).

16. La red de apoyo (Destinos Turísticos Inteligentes – STD)

Fundamentos teóricos para comprender cómo los destinos comparten datos para evitar la masificación y responder a las alertas meteorológicas.

- **Ivars-Baidal, J. A., Celdrán-Bernabeu, M. A. y Mazón, J. N. (2021).** La inteligencia en los destinos turísticos: una perspectiva de gestión y planificación. *Journal of Destination Marketing & Management*, 21. (Explica el uso de la información compartida para la seguridad de los turistas).
- **López de Ávila, A. (2015).** *Destinos inteligentes: innovación de última hora.* Organización Mundial del Turismo. (Autor principal del modelo español de STD, ideal para fundamentar casos como el sistema de «semáforos» de Benidorm).
- **Buhalis, D. (2022).** *Enciclopedia de la gestión y el marketing turístico.* Edward Elgar Publishing. (Contiene las secciones más actualizadas sobre la gobernanza en destinos que utilizan la IA para las alertas meteorológicas).

17. Adaptación climática y gestión de riesgos operativos

Estas fuentes son esenciales para comprender la gestión de desastres y la vulnerabilidad desde una perspectiva sistémica y basada en la comunidad.

- **Centro Internacional de Turismo Sostenible de la APEC. (2007).** *Gestión de riesgos turísticos: una guía de referencia para la gestión de crisis en el turismo.* APEC.

- **Faulkner, B.** (2001). Hacia un marco para la gestión de desastres en el turismo. *Tourism Management*, 22(2), 135-147.
- **Filimonau, V., y De Coteau, D.** (2020). Resiliencia turística en el contexto de la gestión integrada de destinos y desastres (IDDM). *International Journal of Tourism Research*, 22(2), 202-215.
- **García González, E. D., López Guevara, V. M., y López Pardo, G.** (2022). Análisis de la resiliencia social en los sistemas socioecológicos. *Tourism Research*, (23), 48-72.
- **Hall, C. M.** (2010). Crisis y resiliencia en el turismo. *Investigación sobre Turismo y Ocio*, 35(3), 229-245.
- **Ritchie, B. W.** (2004). Caos, crisis y desastres: un enfoque estratégico para la gestión de crisis en la industria turística. *Tourism Management*, 25(6), 669-683.

18. «Transición doble» (transición ecológica y digital)

Marcos estratégicos de la Unión Europea que definen la colaboración necesaria para la transición del sector de cara a 2030.

- **Comisión Europea.** (2019). *El Pacto Verde Europeo*. COM(2019) 640 final.
- **Comisión Europea.** (2020). *Configurar el futuro digital de Europa*.
- **Comisión Europea.** (2022). *Ruta de transición para el turismo*. Documento sobre la transición verde y digital del sector.

19. Economía circular y sostenibilidad en el turismo

Teorías sobre la interdependencia entre las empresas, la comunidad y el medio ambiente para una resiliencia regenerativa.

- **Adger, W. N.** (2000). Resiliencia social y ecológica: ¿están relacionadas? *Progress in Human Geography*, 24(3), 347-364.
- **Berkes, F., Folke, C. y Colding, J.** (2002). *Navegando por los sistemas socioecológicos: desarrollo de la resiliencia ante la complejidad y el cambio*. Cambridge University Press.
- **Fundación Ellen MacArthur.** (s. f.). *La economía circular en los viajes y el turismo*.
- **Naciones Unidas.** (2015). *Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*. Resolución 70/1.

- **Organización Mundial del Turismo (OMT).** (s. f.). *El turismo en la Agenda 2030*.
- **Ostrom, E.** (2009). Un marco general para analizar la sostenibilidad de los sistemas socioecológicos. *Science*, 325(5939), 419-422.

20. Tecnologías digitales para la eficiencia en el uso de los recursos

Fundamentos técnicos para la gestión de riesgos digitales, el factor humano en organizaciones de alta fiabilidad y destinos inteligentes.

- **Glaesser, D.** (2006). *Gestión de crisis en la industria turística*. Elsevier Butterworth-Heinemann.
- **Gretzel, U., Sigala, M., Xiang, Z. y Koo, C.** (2015). Turismo inteligente: fundamentos y desarrollos. *Electronic Markets*, 25(3), 179-188.
- **ISO.** (2018). *Gestión de riesgos — Directrices (ISO 31000:2018)*.
- **SEGITTUR.** (2022). *Guía de destinos turísticos inteligentes*. Ministerio de Industria, Comercio y Turismo.
- **Sutcliffe, K. M.** (2011). Organizaciones de alta fiabilidad (HRO). *Best Practice & Research Clinical Anaesthesiology*, 25(2), 133-144.
- **Weick, K. E. y Sutcliffe, K. M.** (2007). *Gestionar lo inesperado: rendimiento resiliente en una era de incertidumbre*. Jossey-Bass.

21. Gestión estratégica de crisis en el turismo

Estos textos constituyen la base del marco del ciclo de vida de las crisis (prevención, preparación, respuesta, recuperación y aprendizaje) aplicado específicamente al sector.

- **Ritchie, B. W. (2004).** *Caos, crisis y desastres: un enfoque estratégico de la gestión de crisis en la industria turística*. Tourism Management. Se trata de la obra fundamental que define el modelo estratégico para gestionar las perturbaciones en el turismo.
- **Pforr, C. y Hosie, P. J. (2009).** *Gestión de crisis en la industria turística: superar las adversidades*. Ashgate Publishing. Ofrece una visión general exhaustiva de cómo las organizaciones turísticas pueden sobrevivir a desastres naturales y crisis provocadas por el hombre.
- **Glaesser, D. (2006).** *Gestión de crisis en la industria turística internacional*. Routledge. Un manual práctico centrado en la respuesta operativa y la evaluación de riesgos a nivel internacional.

22. Comunicación y recuperación de la reputación

Respalda la teoría sobre la gestión de las reseñas en línea, las relaciones con los medios de comunicación y el restablecimiento de la confianza de los clientes.

- **Coombs, W. T. (2007).** *Comunicación de crisis continua: planificación, gestión y respuesta*. Sage Publications. Lectura imprescindible para comprender la «Teoría de la comunicación de crisis situacional» y cómo proteger el capital reputacional.
- **Benoit, W. L. (1997).** «*El discurso de reparación de la imagen y la comunicación de crisis*». Public Relations Review. Define las estrategias discursivas para reparar la imagen de una organización tras un fallo grave.
- **OMT (2011).** *Guía práctica sobre comunicación en situaciones de crisis en el sector turístico*. Organización Mundial del Turismo. Una guía práctica para destinos y empresas sobre cómo gestionar la comunicación con *las partes interesadas* durante y después de una crisis.

23. Aprendizaje tras la crisis y mejora continua

Esto sustenta el proceso de revisión posterior a la acción (AAR) y el crecimiento postraumático de la organización.

- **Donahue, A. K. y Tuohy, R. V. (2006).** «*Lecciones que no aprendemos: un estudio sobre las lecciones de los desastres, la gestión y la estrategia*». Homeland Security Affairs. Analiza por qué las organizaciones « » suelen fracasar en la fase de aprendizaje y cómo mejorar el proceso de extracción de lecciones.
- **Garvin, D. A. (2000).** *El aprendizaje en acción: una guía para poner en práctica la organización que aprende*. Harvard Business School Press. Proporciona herramientas para convertir la experiencia de una crisis en conocimiento organizativo duradero.

24. Gestión sectorial: salud, clima y riesgos digitales

Referencias específicas para las tres áreas de interés de la unidad.

- **Hall, C. M., Scott, D. y Gössling, S. (2020).** «*Pandemias, transformaciones y turismo: ten cuidado con lo que deseas*». Tourism Geographies. Un análisis en profundidad de la resiliencia ante las crisis sanitarias globales.
- **Becken, S. y Hughey, K. F. (2013).** *La integración del turismo en las estructuras de gestión de emergencias: estructuras y redes de respuesta*. Journal of Sustainable Tourism. Se centra en la respuesta a los desastres relacionados con el clima y en la integración con las autoridades públicas.



 treadsproject.eu

 [treads-project](https://www.linkedin.com/company/treads-project)

 [Treads Project](https://www.facebook.com/TreadsProject)

 [treadsprojecteu](https://www.instagram.com/treadsprojecteu)



Co-funded by the
European Union

Co-funded by the European Union. The opinions and views expressed are solely those of the author(s) and do not necessarily reflect those of the European Union or the Spanish Service for the Internationalization of Education (SEPIE). Neither the European Union nor the granting authority can be held responsible for them