



Unidad formativa 2:

Seguridad Digital en el Turismo

Tourism Resilience Education in Digital Security



Co-funded by
the European Union

ÍNDICE

INTRODUCCIÓN	3
UNIDAD FORMATIVA 2: SEGURIDAD DIGITAL EN EL TURISMO	4
Objetivos del curso	4
Resultados de aprendizaje	4
Estructura y metodología de la unidad	5
2.1 Fundamentos de la seguridad digital	7
1.	7
2.	11
3.	14
4.	18
5.	22
6.	25
7.	29
8.	33
2.2 Seguridad en los procesos turísticos digitales	36
1.	41
2.	46
3.	51
4.	55
5.	57
6.	61
7.	64
8.	68
2.3 Simulaciones y gestión de crisis digitales	62
1.	71
2.	73

- 3. 74
- 4. 78
- 5. 80
- 6. 83
- 7. 85

REFERENCIAS

80

LISTA DE FIGURAS

Figura 1: Flujo de datos turísticos y vulnerabilidades en las OTA, los CRS, los PMS y los sistemas de pago	8
Figura 2: Cadena de ataque de ingeniería social	17
Figura 3: Fases clave de respuesta durante las primeras 24 horas tras una filtración de datos	51

El proyecto TREADS responde a la acelerada transformación digital del sector turístico europeo, prestando especial atención a las microempresas y pymes que constituyen la columna vertebral de la industria. Si bien la digitalización mejora la competitividad y la eficiencia operativa, también conlleva riesgos significativos relacionados con la gestión de datos, la ciberseguridad y la desinformación. El sector turístico se encuentra entre las industrias más atacadas por los ciberataques, lo que pone de relieve la urgente necesidad de una educación y formación estructuradas que refuercen la resiliencia digital.

Al mismo tiempo, el Pacto de la UE por las Competencias en el Turismo identifica un déficit persistente de competencias en el sector, especialmente entre los operadores a pequeña escala, donde las competencias digitales y de ciberseguridad siguen estando desarrolladas de forma desigual. Abordar este déficit es esencial para garantizar una transición segura y sostenible hacia la era digital.

En este marco, el presente documento constituye el plan de estudios estructurado para la Unidad de Formación 2: *Seguridad digital en el turismo*, y está diseñado para impartirse como un curso de Educación y Formación Profesional (EFP) de 48 horas. El curso se centra en la seguridad digital en el turismo y abarca los procesos turísticos digitales y la gestión de crisis digitales mediante una combinación de fundamentos teóricos, conocimiento de la normativa, ejercicios prácticos y aprendizaje basado en simulaciones. Se ajusta a los marcos normativos pertinentes de la UE y tiene como objetivo dotar a los formadores y alumnos de la EFP de competencias prácticas que mejoren la resiliencia organizativa, las prácticas digitales responsables y la respuesta estructurada ante crisis en el ecosistema turístico.

UNIDAD FORMATIVA 2: SEGURIDAD DIGITAL EN EL TURISMO

Objetivos del curso

Esta unidad formativa tiene como objetivo reforzar la capacidad de los profesionales del turismo para operar de forma segura en entornos interconectados digitalmente. Proporciona los conocimientos estructurados, las habilidades operativas aplicadas y la sensibilización orientada a la gobernanza necesarios para gestionar los riesgos digitales en los procesos turísticos.

La unidad pretende:

- Sensibilizar sobre los riesgos digitales sistémicos en los ecosistemas turísticos interconectados;
- Reforzar las prácticas operativas seguras en la gestión de los datos de los clientes, los pagos y los sistemas de reserva;
- Armonizar el comportamiento profesional con las políticas de seguridad de la organización y los requisitos normativos de la UE;
- Reforzar los procedimientos estructurados de escalación y la respuesta coordinada ante incidentes;
- Fomentar la resiliencia digital y mantener la confianza de los clientes en las organizaciones turísticas.

El objetivo general de esta unidad es apoyar el desarrollo de profesionales del turismo con competencias digitales que combinen los conocimientos técnicos con un comportamiento responsable y una respuesta estructurada ante incidentes.

Resultados del aprendizaje

CONOCIMIENTOS

Al finalizar la formación, el alumno será capaz de describir conceptos básicos de seguridad digital y comprender las amenazas digitales más comunes que afectan al sector turístico. Reconocerá las vulnerabilidades típicas de los procesos turísticos digitales, como los sistemas de reserva en línea, los pagos digitales y las prácticas de gestión de datos. El alumno también comprenderá los principios fundamentales de la seguridad digital, incluido el concepto de «seguridad de confianza cero» (Zero Trust Security), y será capaz de identificar los requisitos normativos básicos relacionados con la protección de datos y la seguridad digital, como el Reglamento General de Protección de Datos (RGPD). Además, comprenderá cómo los incidentes digitales pueden afectar a la continuidad del negocio y a la reputación de las organizaciones turísticas.

COMPETENCIAS

El alumno será capaz de aplicar prácticas básicas de seguridad digital en las operaciones turísticas diarias y de seguir procedimientos seguros al gestionar datos de clientes, reservas en línea y sistemas de pago digital. Será capaz de detectar y notificar actividades digitales sospechosas, como intentos de phishing o fraude en línea, y de responder adecuadamente a ciberincidentes simulados, incluidas las filtraciones de datos o los ataques de ransomware. Además, los alumnos podrán contribuir a los procedimientos de comunicación interna y de respuesta durante las crisis digitales.

COMPETENCIAS

El alumno trabajará de forma responsable con los sistemas digitales y los datos de los clientes, de acuerdo con las políticas de seguridad establecidas. Apoyará las respuestas de la organización ante incidentes de seguridad digital dentro de su ámbito de responsabilidad y será capaz de adaptar su comportamiento y sus procedimientos con el fin de reducir los riesgos digitales en entornos turísticos.

Estructura y metodología de la unidad

DURACIÓN

48 horas (16 por cada subunidad)

MÉTODOS DE IMPARTICIÓN

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

ACTIVIDADES PRÁCTICAS Y RESULTADOS RELACIONADOS

- Evaluación básica de seguridad de una página web relacionada con el turismo, en la que se identifiquen posibles vulnerabilidades relacionadas con la protección de datos, las reservas en línea y el acceso de los usuarios. Posteriormente, se elaborará un breve informe de auditoría de seguridad en el que se describirán los riesgos identificados y las medidas de mitigación recomendadas
- Caso práctico sobre un ataque de ransomware a un sistema de gestión hotelera (PMS). Los alumnos analizarán un caso práctico realista centrado en las causas, las repercusiones y las medidas de respuesta, y redactarán un análisis del caso en el que describirán el incidente, la estrategia de respuesta y las lecciones aprendidas
- Taller sobre planificación de la comunicación ante crisis por fugas de datos: mediante trabajo en grupo, los alumnos diseñarán y redactarán un plan de comunicación que aborde la comunicación interna y externa durante una fuga de datos o un incidente de seguridad digital, y presentarán su trabajo al formador y al resto de alumnos
- Simulacros de ataques de phishing y escenarios de fraude en reservas en línea, seguidos de una lista de verificación que recoja las respuestas correctas y las áreas de mejora
- Elaboración de un plan integral de seguridad digital para una agencia de turismo o un hotel, que incluya medidas preventivas, procedimientos de respuesta y funciones

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

EVALUACIÓN

- Breves cuestionarios sobre conocimientos teóricos
- Evaluación de las actividades prácticas mediante, por ejemplo, cuestionarios, pruebas, hackatones, informes, listas de verificación y presentaciones en grupo

El rendimiento del alumno se evaluará en función de su capacidad para identificar correctamente los riesgos de seguridad digital en situaciones prácticas relacionadas con el turismo. Se espera que demuestre el uso seguro de las herramientas digitales

durante simulaciones o ejercicios prácticos, así como que complete con éxito simulaciones de detección de phishing o fraude.

La evaluación también tendrá en cuenta la contribución del alumno al desarrollo de un plan básico de respuesta a incidentes digitales o de comunicación. Por último, los alumnos deberán superar las evaluaciones finales que combinan los conocimientos teóricos con la aplicación práctica.

2.1 Fundamentos de la seguridad digital

Al finalizar la subunidad, los alumnos serán capaces de reconocer comportamientos digitales inseguros, aplicar normas básicas de seguridad en el trabajo diario, notificar incidentes correctamente y comprender las funciones y responsabilidades.

- Conceptos básicos de seguridad digital
 - Ciberhigiene (gestión de contraseñas, autenticación multifactorial, actualizaciones, copias de seguridad)
 - El factor humano en la seguridad digital
 - Marco normativo (conceptos básicos del RGPD para el personal turístico), Directiva NIS2 (visión general, relevancia para la cadena de suministro turística)
- Amenazas digitales más comunes en el sector turístico
- Desinformación e ingeniería social dirigidas a las empresas turísticas (opiniones falsas, alertas falsas, comunicaciones manipuladas con los clientes)
- Introducción a la seguridad «Zero Trust»

Actividad práctica sugerida:

- Cuestionario de concienciación sobre seguridad digital

1. Por qué la seguridad digital es fundamental en el turismo

La seguridad digital desempeña un papel fundamental en el sector turístico, donde las organizaciones recopilan y procesan continuamente datos personales y de pago

en entornos digitales interconectados. Los sistemas de reservas, las plataformas en línea y los servicios de pago intercambian datos en tiempo real para permitir las reservas, los registros de llegada y las transacciones financieras. Los elevados volúmenes de transacciones, la gran dependencia de socios externos y la accesibilidad permanente a los sistemas amplían significativamente la superficie de ataque, lo que aumenta la exposición a errores operativos, usos indebidos y ciberataques. Dado que estos sistemas están estrechamente conectados, incluso una pequeña vulnerabilidad en una parte de la cadena digital puede tener consecuencias de gran alcance para los huéspedes, el personal y las operaciones empresariales.

Entre los sistemas clave que intervienen en este flujo de datos se incluyen:

- **Sistemas de gestión hotelera (PMS):** sistemas internos del hotel utilizados para reservas, registros de entrada, registros de huéspedes y facturación;
- **Sistemas centrales de reservas (CRS):** sistemas que sincronizan la disponibilidad de habitaciones y los precios en múltiples canales de reserva;
- **Plataformas de pago:** herramientas que procesan pagos con tarjeta, reembolsos y devoluciones.

Dado que estos sistemas están interconectados, una vulnerabilidad en uno de ellos puede afectar a los demás. Un incidente típico sigue una cadena predecible:



Por ejemplo, en incidentes reales, los hoteles que siguieron aceptando pagos sin **3-D Secure** (un paso de verificación adicional para los titulares de tarjetas) durante interrupciones importantes del sistema se enfrentaron posteriormente a un aumento de las devoluciones y a pérdidas económicas. Ese riesgo es la razón por la que la normativa de la UE sobre el intercambio fiable de datos y la rendición de cuentas —en particular, la Ley de Gobernanza de Datos¹— promueve mecanismos

¹ Parlamento Europeo y Consejo de la Unión Europea. (2022). *Reglamento (UE) 2022/868, de 30 de mayo de 2022, sobre la gobernanza de los datos en Europa y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de gobernanza de los datos)*. Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868>

Unidad formativa 2: Seguridad digital en el Turismo

para «facilitar el intercambio de datos entre sectores», al tiempo que aumenta la confianza en el tratamiento de los datos.

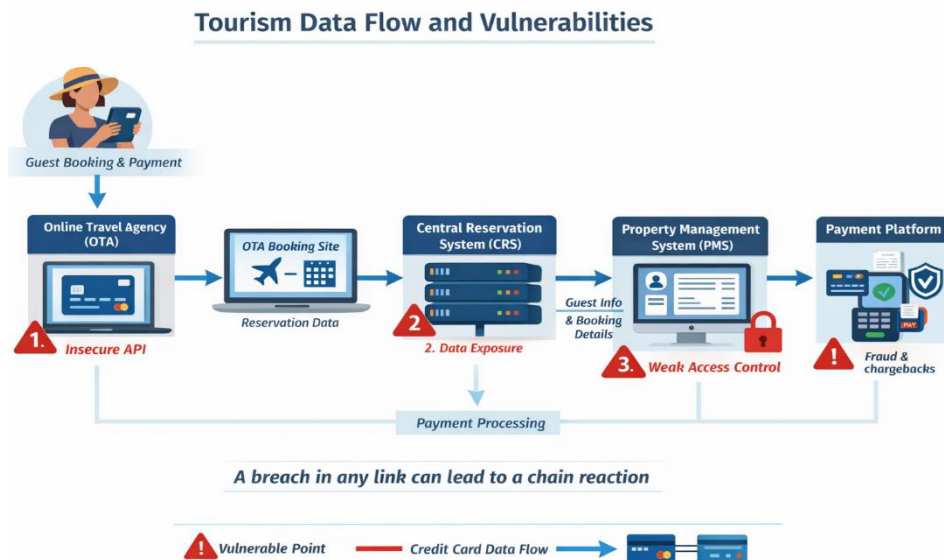


Figura 1: Flujo de datos turísticos y vulnerabilidades en las OTA, los CRS, los PMS y los sistemas de pago

El sector turístico está especialmente expuesto debido a que los datos se comparten constantemente entre socios. Una sola **API** expuesta —una interfaz digital que permite la comunicación entre diferentes sistemas de software— en una **agencia de viajes en línea (OTA)** puede permitir a los atacantes acceder a grandes volúmenes de datos de reservas. Una vez que los atacantes logran afianzarse, pueden desplazarse a través de los sistemas vinculados y provocar fallos en cadena que afecten a múltiples organizaciones. La dimensión ética de la protección de los viajeros y sus datos también se destaca explícitamente en el **Código Ético Mundial para el Turismo de la OMT²**, que insta a que «las partes interesadas públicas y privadas en el desarrollo del turismo cooperen en la aplicación de estos principios» (responsabilidades de aplicación y cooperación).

Estos incidentes provocan daños en el mundo real. Los huéspedes pueden sufrir fraudes o el uso indebido de su identidad, el personal debe dedicar tiempo a gestionar los incidentes en lugar de atender a los clientes, y las organizaciones sufren perjuicios económicos y de reputación. La responsabilidad ética de proteger a los huéspedes también se destaca en el **Código Ético Mundial para el Turismo de la OMT**, que establece que los agentes del sector turístico deben garantizar la protección de los turistas y de sus datos personales.

² Organización Mundial del Turismo (OMT). (s. f.). *Código ético mundial del turismo*. <https://www.untourism.int/global-code-of-ethics-for-tourism>

Más allá

Los riesgos de seguridad digital varían según el modelo de negocio:

- **Los hoteles** se centran en proteger los perfiles concentrados de los huéspedes y en mantener unas operaciones diarias ininterrumpidas. Los incidentes suelen tener un impacto operativo inmediato, que afecta al registro de entrada, a la facturación y a la experiencia de los huéspedes.
- **Las organizaciones de promoción de destinos (DMO)** dependen de conjuntos de datos compartidos y de fuentes de información de socios, lo que las hace vulnerables a información corrupta, retrasada o engañosa que puede afectar a la reputación del destino y a la toma de decisiones.
- Las **agencias de viajes en línea (OTA)** centralizan las reservas de miles de proveedores e integran a numerosos socios a través de interfaces técnicas. Están especialmente expuestas al riesgo sistémico relacionado con las API, en el que una sola vulnerabilidad puede propagarse simultáneamente a múltiples organizaciones.

Abordar estos riesgos requiere el desarrollo de la mano de obra y de las competencias digitales: la asociación para las competencias turísticas, en el marco del Pacto de la UE por las Competencias, tiene como objetivo promover la mejora de las competencias y el reciclaje profesional del 60 % de la mano de obra cada año hasta 2030 en todo el ecosistema³, lo que contribuye directamente a mejorar la concienciación cibernética y la resiliencia operativa.

Reflexión y debate

³ Comisión Europea. (2024). *El Pacto de la UE por las Competencias: Alianza para las Competencias en el Ecosistema Turístico (Actualización de la situación de partida)*. Comisión Europea.
https://pact-for-skills.ec.europa.eu/document/download/83968c43-1706-4fbd-9fd0-4461583607d7_en?filename=Pact%20for%20Skills%20Tourism%20Baseline%20-%20update%2020240229.pdf

01

¿Por qué se considera el turismo un sector de alto riesgo para la seguridad digital?

02

Nombra dos consecuencias de un incidente digital y explica una de ellas.

03

Más allá: ¿Qué modelo de negocio está más expuesto a los riesgos derivados de las API inseguras y por qué?

2. Conceptos básicos de ciberseguridad

El riesgo de seguridad digital sigue una lógica sencilla y repetible que se aplica a la mayoría de las organizaciones y sistemas. En la mayoría de los casos, los atacantes comienzan identificando debilidades comunes y fácilmente explotables, en lugar de utilizar técnicas muy sofisticadas. Entre los ejemplos típicos se incluyen contraseñas débiles o reutilizadas, configuraciones incorrectas del sistema y actualizaciones de software pendientes.

Cuando se aprovecha una de estas vulnerabilidades, el impacto rara vez se limita a un único sistema. Las consecuencias pueden incluir rápidamente la pérdida de datos personales o empresariales, la interrupción de los servicios, el fraude financiero y los costes adicionales de recuperación relacionados con la investigación, la corrección y la pérdida de productividad. Comprender esta lógica de causa y efecto es esencial para reconocer cómo pequeñas debilidades pueden derivar en importantes problemas operativos y empresariales.

En el ámbito del turismo, los riesgos suelen clasificarse en dos **categorías que interactúan entre sí**:

- **Riesgos técnicos**, como interfaces de sistema (API) inseguras, servidores obsoletos, servicios mal configurados y parches de seguridad que faltan.
- **Riesgos de origen humano**, como el phishing, el uso indebido de credenciales o la exposición accidental de datos personales.

Estos riesgos se refuerzan mutuamente. Por ejemplo, un solo correo electrónico de phishing puede engañar a un miembro del personal para que revele sus credenciales, lo que a su vez permite a un atacante aprovechar una vulnerabilidad técnica existente. Del mismo modo, un fallo técnico puede generar confusión o una sensación de urgencia que los atacantes aprovechan para manipular el comportamiento humano.

El «Zero Trust» como principio práctico de seguridad

Para reducir la propagación de incidentes, un principio de seguridad ampliamente utilizado es el «Zero Trust». En lugar de dar por sentado que los usuarios o los sistemas son fiables por defecto, el acceso solo se concede tras una verificación. Los elementos fundamentales de este enfoque incluyen la verificación de la identidad, la limitación del acceso a lo estrictamente necesario, la separación de los sistemas siempre que sea posible y la supervisión de la actividad para detectar anomalías.

En la práctica, el «Zero Trust» ayuda a garantizar que el compromiso de una cuenta o un sistema no conduzca automáticamente a un acceso generalizado en todos los entornos conectados. Esto resulta especialmente importante en el sector turístico, donde los sistemas están estrechamente integrados y las funciones del personal cambian con frecuencia.

Medidas prácticas de mitigación

A este nivel, las medidas de mitigación eficaces son sencillas y aplicables:

- aplicar actualizaciones de software y parches de seguridad periódicamente para subsanar las vulnerabilidades conocidas antes de que puedan ser explotadas;
- utilizar métodos de autenticación sólidos y el principio del «privilegio mínimo», de modo que los usuarios solo puedan acceder a los sistemas y datos necesarios para su función;
- registrar y supervisar comportamientos sospechosos, manteniendo registros de las acciones importantes del sistema y comprobando si se producen actividades inusuales;
- formar al personal para que reconozca el phishing y otras técnicas de ingeniería social, de modo que los mensajes o solicitudes sospechosos se identifiquen y notifiquen a tiempo.

En conjunto, estas medidas reducen tanto los riesgos técnicos como los derivados del factor humano y ayudan a limitar los daños cuando se produce un incidente.

Escenario: Verificación bajo presión

Una celebridad muy conocida se aloja en su destino. Una persona llama a la recepción del hotel, afirmando ser el «asistente personal» del huésped, y solicita el

número de habitación y una copia del folio de registro de entrada «a efectos fiscales».

Esta situación plantea cuestiones importantes:

- **El dilema:** ¿Aplicar el modelo «Zero Trust» significa sospechar de todo el mundo, incluso a riesgo de ofender a un VIP?
- **El reto de la cooperación:** ¿Cómo puede el personal verificar la identidad de la persona que llama a través de los canales adecuados sin parecer descortés ni menoscabar la experiencia de hospitalidad?

Este escenario pone de relieve cómo deben aplicarse los principios de seguridad de manera que se respeten tanto los requisitos de protección como la cultura del servicio turístico.

Más allá

El modelo «Zero Trust» es eficaz desde el punto de vista conceptual, pero los sistemas más antiguos o heredados suelen carecer de capacidades integradas de gestión de identidades o de segmentación de accesos. En dichos entornos, las organizaciones recurren a **controles compensatorios**, como la autenticación en la puerta de enlace, la segmentación de la red y el registro mejorado de actividades, para reducir la exposición. Planificar actualizaciones por fases junto con medidas de protección provisionales es esencial para gestionar el riesgo de forma eficaz y, al mismo tiempo, evitar la interrupción de las operaciones diarias.

El «Zero Trust» debe entenderse como un enfoque de seguridad a largo plazo, más que como una tecnología aislada o una solución rápida.

Reflexión y debate

01

¿Cuál es la diferencia entre una amenaza y una vulnerabilidad?

02

Da dos ejemplos de riesgos provocados por el factor humano y describe una medida sencilla para mitigarlos.

03

Más allá: ¿Cuál es la principal limitación a la hora de aplicar el modelo «Zero Trust» a los sistemas heredados?

3. Higiene cibernética en los lugares de trabajo del sector turístico

La mayoría de los incidentes digitales no comienzan con la intrusión de hackers, sino con rutinas de trabajo cotidianas. El comportamiento habitual en el día a día influye en gran medida en que los pequeños problemas sigan siendo menores o se conviertan en incidentes digitales graves.

Entre los descuidos cotidianos más habituales se incluyen:

- el uso de contraseñas débiles o reutilizadas (por ejemplo, 123456, «contraseña»);
- posponer o ignorar las actualizaciones de software;
- dejar sesiones sin cerrar en dispositivos compartidos en recepción o en la oficina administrativa;
- guardar contraseñas en los navegadores de ordenadores comunes;
- utilizar redes Wi-Fi públicas no seguras para tareas relacionadas con el trabajo.

En las organizaciones turísticas, donde se manejan a diario datos personales y de pago, estos descuidos aparentemente insignificantes pueden dar lugar rápidamente a la exposición de datos, a transacciones fraudulentas o a interrupciones del servicio.

Medidas prácticas y de gran impacto

Las medidas prácticas y de gran impacto se centran en reducir los riesgos digitales cotidianos. Son más eficaces cuando son fáciles de aplicar y se siguen de forma sistemática. En lugar de depender de tecnología avanzada, estas medidas se centran en la prevención y la limitación temprana de los daños mediante el refuerzo de los hábitos cotidianos, los controles de acceso y la higiene básica de los sistemas.

Entre las medidas clave se incluyen:

- **Utilizar contraseñas seguras y únicas** para cada sistema (por ejemplo, BlueCoffee-Flying-Moon!77) y almacenarlas de forma segura en un gestor de contraseñas, cuando esté disponible. Las contraseñas deben cambiarse inmediatamente si se sospecha que han sido comprometidas, tras un incidente de seguridad, cuando las credenciales puedan haber quedado expuestas o cuando la política de la organización así lo exija. Por lo general,

no se recomienda cambiar las contraseñas de forma rutinaria sin que haya indicios de que hayan sido comprometidas, ya que esto puede fomentar prácticas de contraseñas más débiles y la reutilización de contraseñas.

- **Habilitar la autenticación multifactorial (MFA)** para añadir una capa adicional de protección y evitar la apropiación de cuentas, incluso si se roban las contraseñas;
- **Aplicar actualizaciones de software y parches de seguridad periódicamente** para subsanar las vulnerabilidades conocidas antes de que puedan ser aprovechadas.

Gestión de riesgos en dispositivos compartidos y teletrabajo

Los dispositivos compartidos suponen un riesgo específico en los lugares de trabajo del sector turístico, donde varios miembros del personal utilizan los mismos sistemas a lo largo de los turnos. Dado que las acciones de los distintos usuarios se mezclan, resulta más difícil determinar la responsabilidad y más fácil que el acceso no autorizado pase desapercibido.

Entre las medidas de mitigación sencillas y eficaces se incluyen:

- bloquear las pantallas al alejarse de un puesto de trabajo;
- utilizar cuentas de usuario individuales para cada miembro del personal;
- evitar el almacenamiento de contraseñas en los navegadores de los ordenadores comunes.

El teletrabajo seguro requiere un cuidado adicional. El personal debe utilizar redes de confianza o una VPN y evitar las redes Wi-Fi públicas al realizar tareas confidenciales.

Seguridad de los dispositivos móviles en el sector turístico

Los dispositivos móviles se han convertido en parte del trabajo diario en el sector turístico. El personal suele utilizar smartphones y tabletas para acceder al correo electrónico, a plataformas de reservas, a sistemas de pago, a información de clientes y a herramientas de comunicación.

Si se pierde, roban o se ve comprometido un dispositivo, personas no autorizadas podrían acceder a los sistemas de la empresa o a datos confidenciales de los clientes.

Por este motivo, **los dispositivos móviles deben protegerse de la misma forma que los ordenadores y otros sistemas del lugar de trabajo.**

Entre las buenas prácticas se incluyen:

- utilizar un bloqueo de pantalla (PIN, contraseña, huella dactilar o reconocimiento facial);
- activar la autenticación multifactorial (MFA) cuando sea posible;
- mantener los dispositivos y las aplicaciones con los últimos parches de seguridad y actualizaciones de software;
- descargar aplicaciones únicamente de fuentes fiables;
- notificar lo antes posible la pérdida o el robo de dispositivos;
- evitar el acceso a información confidencial a través de redes Wi-Fi públicas no seguras.

Estas sencillas precauciones pueden reducir significativamente el riesgo de acceso no autorizado y ayudar a proteger tanto la información de la organización como la de los clientes.

Fomentar hábitos seguros mediante la formación

La formación desempeña un papel fundamental a la hora de convertir las medidas de seguridad en hábitos constantes. El personal debe comprender cómo los ataques de phishing e ingeniería social se aprovechan de comportamientos rutinarios, como hacer clic en enlaces o introducir credenciales bajo presión.

Una formación eficaz se centra en:

- reconocer mensajes y solicitudes sospechosos;
- saber cuándo y cómo notificar posibles incidentes;
- poner en práctica los pasos de escalado para que los problemas se resuelvan rápidamente.

En conjunto, estos controles prácticos reducen significativamente la probabilidad de que un simple error —como hacer clic en un enlace malicioso o dejar una sesión sin

cerrar— se convierta en un incidente grave que perjudique a los huéspedes o sobrecargue al personal.

Métodos de autenticación emergentes: las claves de acceso

Las claves de acceso son un método de autenticación emergente diseñado para sustituir a las contraseñas tradicionales. En lugar de basarse en credenciales memorizadas, las claves de acceso utilizan claves criptográficas almacenadas de forma segura en un dispositivo de confianza y, por lo general, se desbloquean mediante datos biométricos (como el reconocimiento de huellas dactilares o facial) o el PIN del dispositivo.

Entre sus principales ventajas se incluyen:

- resistencia a los ataques de phishing;
- la eliminación de la reutilización de contraseñas;
- mejora de la experiencia del usuario;
- mayor protección contra la apropiación de cuentas.

Los principales proveedores de tecnología, como Apple, Google y Microsoft, admiten cada vez más las claves de acceso tanto en servicios para consumidores como para empresas. A medida que su adopción sigue creciendo, las organizaciones turísticas pueden encontrarse con la autenticación basada en claves de acceso en sistemas de reservas, plataformas en la nube y aplicaciones orientadas al cliente.

Más allá

El diseño de las políticas debe encontrar un equilibrio entre la seguridad y la practicidad. Las normas excesivamente estrictas y engorrosas —como la rotación obligatoria y constante de contraseñas o una autenticación excesivamente compleja para tareas básicas— pueden reducir el cumplimiento por parte del personal. Por el contrario, unos controles demasiado laxos aumentan la exposición al riesgo. El enfoque más eficaz utiliza controles específicos, excepciones claras y procedimientos sencillos, lo que permite al personal adoptar hábitos de protección de forma coherente como parte de su trabajo diario.

Reflexión y debate

01

¿Cuáles son las tres acciones rutinarias que más reducen el riesgo de apropiación de cuentas y por qué?

02

Indica un riesgo asociado a los dispositivos compartidos y una medida sencilla para mitigarlo.

03

Más allá: ¿Por qué una política de ciberhigiene debe equilibrar la seguridad y la practicidad?

4. El factor humano, la ingeniería social y la desinformación

Los ataques centrados en las personas se aprovechan de **la confianza y los comportamientos rutinarios**, más que de las debilidades técnicas. Los correos electrónicos de phishing, las llamadas de suplantación de identidad y las solicitudes falsas de proveedores se basan en mensajes creíbles para engañar al personal y que este comparta credenciales, apruebe pagos o revele información confidencial. En el sector turístico, los atacantes suelen hacerse pasar por socios, plataformas o compañeros de trabajo conocidos para crear una sensación de urgencia y eludir los pasos de verificación habituales.

La lógica de estos ataques es sencilla y repetible:

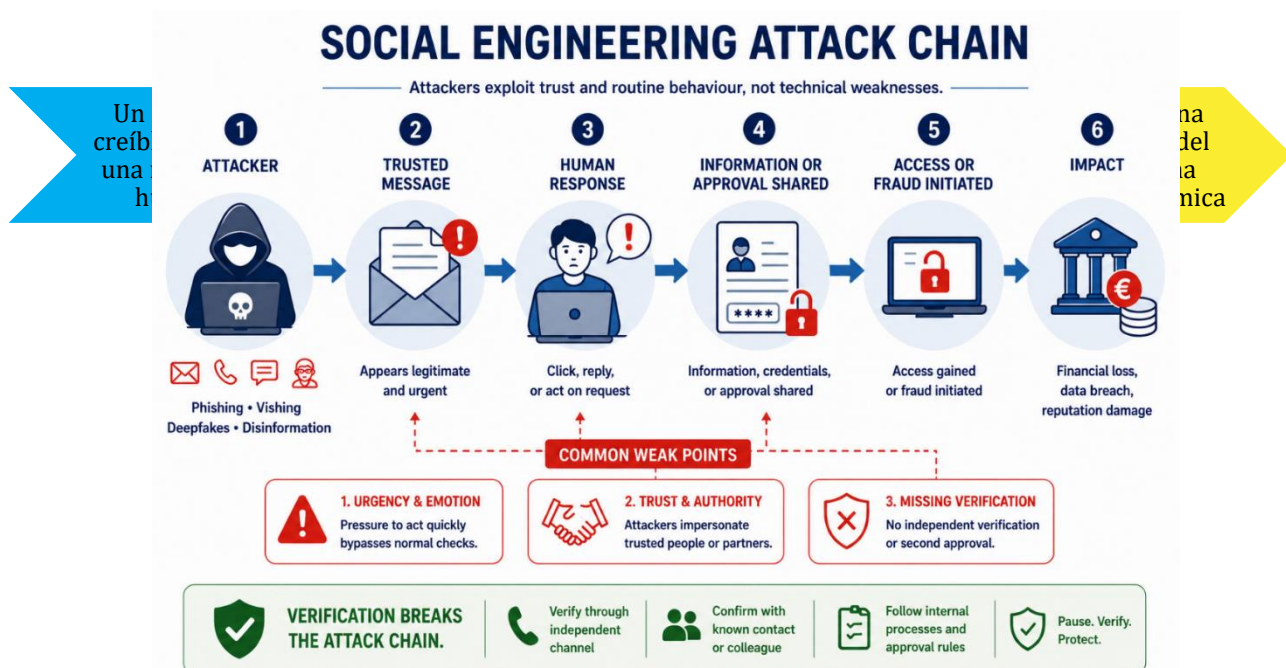


Figura 2: Cadena de ataque de ingeniería social

Escenario práctico: solicitud urgente de un proveedor

Un contable de un hotel recibe un correo electrónico que parece proceder de un proveedor con el que lleva trabajando mucho tiempo, en el que se solicita un cambio urgente en los datos de la cuenta bancaria. El mensaje utiliza un lenguaje familiar e incluye una factura que parece auténtica. Dado que la solicitud está marcada como urgente y el remitente parece de confianza, el contable se siente presionado a actuar con rapidez para evitar retrasos en el pago.

Utiliza la siguiente lista de comprobación para evaluar la situación:

- ✓ ¿La solicitud es urgente o está formulada de manera que apele a las emociones?
- ✓ ¿Implica dinero, acceso o datos confidenciales?
- ✓ ¿El remitente te resulta familiar y te inspira confianza?
- ✓ ¿Se puede verificar la solicitud a través de un canal de contacto conocido y ya existente?
- ✓ ¿Es necesaria una segunda aprobación o confirmación interna?
- ✓ ¿La solicitud elude los pasos habituales de aprobación o revisión?
- ✓ ¿Hay pequeñas inconsistencias (nombres, firmas, números de factura, formato)?
- ✓ ¿El mensaje ejerce presión para actuar de inmediato sin dar tiempo a verificarlo?
- ✓ Si esta solicitud fuera fraudulenta, ¿cuál sería el posible impacto en el dinero, los datos o la reputación?

Desinformación e ingeniería social en el sector turístico

La desinformación añade un nivel adicional de riesgo a los ataques de ingeniería social. Las alertas falsas, las reseñas en línea manipuladas o los mensajes de clientes falsificados pueden inducir a error tanto al personal como a los huéspedes, provocar acciones innecesarias y socavar la confianza en los sistemas y las organizaciones.

Entre las señales de alerta más comunes de los intentos de ingeniería social se incluyen:

- un lenguaje urgente o cargado de emotividad;
- solicitudes inesperadas relacionadas con pagos o acceso;
- direcciones de remitente que no coinciden o son inusuales;

- pequeñas inconsistencias ortográficas, de formato o de tono.

La medida defensiva más fiable es **la verificación**. Las solicitudes sospechosas deben confirmarse a través de un canal independiente, como llamar a un número de contacto conocido o comprobarlo internamente. En el caso de acciones financieras o delicadas, exigir una segunda aprobación reduce significativamente el riesgo.

Romper la cadena de ataque

Los procesos bien diseñados pueden interrumpir los ataques de ingeniería social en una fase temprana. Exigir una verificación antes de actuar, separar funciones (por ejemplo, que sean personas diferentes las que inicien y aprueben las transacciones) y definir vías de escalación claras reducen drásticamente el daño potencial. Estos controles son eficaces incluso sin necesidad de modificar los sistemas técnicos centrales.

Una cultura de verificación prudente, combinada con controles sencillos de las transacciones, dificulta mucho más que los atacantes conviertan un contacto inicial en un fraude o en una pérdida de datos.

Ejemplo real: incidente de ransomware notificado que afectó a una cadena hotelera europea⁴

En **octubre de 2023**, el grupo hotelero europeo **Motel One** reveló que había sido víctima de un ataque de ransomware atribuido al grupo cibercriminal **ALPHV/BlackCat**. Según la información pública, el incidente implicó **el acceso no autorizado a datos relacionados con los clientes, incluida la información de reservas y los datos de contacto** (SecurityWeek, 2023).

Aunque la empresa afirmó que las operaciones hoteleras seguían funcionando con normalidad, el ataque suscitó preocupación por la posible exposición de datos personales y tuvo repercusiones normativas y reputacionales. Como suele observarse en los incidentes de ransomware, los autores de la amenaza publicaron en Internet afirmaciones sobre el volumen de datos supuestamente sustraídos; sin embargo, dichas afirmaciones pueden exceder la información confirmada oficialmente y deben interpretarse con cautela mientras las investigaciones siguen en curso.

⁴ Security Week (octubre de 2023). *Motel One revela un ataque de ransomware que ha afectado a los datos de sus clientes*. <https://www.securityweek.com/motel-one-discloses-ransomware-attack-impacting-customer-data/>

El caso ilustra cómo las deficiencias en los controles de acceso administrativo y en la seguridad de la red pueden dar lugar a una exposición de datos a gran escala en el sector hotelero. Incluso cuando los servicios básicos siguen operativos, los incidentes de ransomware pueden generar interrupciones operativas, repercusiones financieras, escrutinio regulatorio y daños a la reputación a largo plazo.

Este ejemplo refuerza la naturaleza sistémica del riesgo digital en los ecosistemas turísticos, donde los sistemas interconectados de reservas, pagos y gestión de relaciones con los clientes (CRM) aumentan el impacto potencial de los ciberincidentes en las dimensiones operativa, financiera y normativa.

Ingeniería social potenciada por la IA

Los ataques de ingeniería social recurren cada vez más a la inteligencia artificial para crear comunicaciones fraudulentas más convincentes y personalizadas. En el pasado, los mensajes de phishing solían ser más fáciles de identificar porque contenían errores ortográficos, expresiones inusuales u otros indicios que sugerían que no eran auténticos. Hoy en día, las herramientas de IA pueden generar correos electrónicos, mensajes, grabaciones de audio e incluso vídeos de aspecto profesional que se asemejan mucho a las comunicaciones legítimas.

- Correos electrónicos de phishing generados por IA;
- ataques de clonación de voz (vishing);
- suplantación de identidad mediante vídeos «deepfake»;
- mensajes falsos de clientes generados por herramientas de IA;
- ataques de inyección de comandos dirigidos a los sistemas de IA utilizados en las organizaciones;

Estas técnicas dificultan la verificación, ya que los atacantes pueden imitar a personas u organizaciones de confianza con un alto grado de credibilidad. Se puede suplantar la identidad de directivos, proveedores, compañeros de trabajo, socios comerciales o clientes con el fin de obtener información, acceder a los sistemas o persuadir al personal para que realice acciones que normalmente no llevaría a cabo. Por ello, las organizaciones deben prestar mayor atención a los procedimientos de verificación y a la confirmación independiente de solicitudes inusuales, incluso cuando las comunicaciones parezcan auténticas.

Ejemplo real: suplantación de identidad de un ejecutivo mediante deepfake⁵

En 2024, una empresa multinacional de ingeniería fue objeto de un ataque en el que los atacantes utilizaron tecnología «deepfake» durante una videoconferencia para suplantar a altos ejecutivos. Al creer que la reunión era auténtica, un empleado autorizó una serie de transacciones que provocaron pérdidas de aproximadamente 25 millones de dólares estadounidenses. **Más allá**

Al analizar la cadena de ataque de ingeniería social (reconocimiento → contacto → explotación → retirada de fondos), la mayor ventaja radica en bloquear las primeras etapas. Una verificación de identidad sólida, controles estrictos de aprobación de transacciones y pasos de confirmación obligatorios limitan significativamente el margen de maniobra de los atacantes y reducen el impacto posterior. Estas medidas siguen siendo eficaces incluso cuando aún no es factible llevar a cabo actualizaciones técnicas completas.

Reflexión y debate

01

¿Qué tácticas habituales utilizan los atacantes para engañar al personal y cuál es una de las consecuencias directas?

02

Nombra dos señales de alerta de un mensaje fraudulento y una medida de seguridad que se pueda tomar.

03

Más allá: ¿Qué puntos de la cadena de ataque de ingeniería social son más eficaces de bloquear y por qué?

5. Fundamentos normativos: el RGPD y la NIS2 en el turismo

La protección de datos y la seguridad digital en el sector turístico se rigen por dos marcos normativos clave: **el RGPD**, que se centra en la protección de los datos personales y los derechos individuales, y **la NIS2**, que se centra en la resiliencia de los servicios digitales y la seguridad de la cadena de suministro.

En virtud **del RGPD**, las organizaciones están obligadas a proteger los datos personales mediante medidas como la minimización de datos, los controles de acceso y la notificación oportuna de las violaciones de seguridad. **El Reglamento**

⁵ CNN (2024). *Un empleado del departamento financiero paga 25 millones de dólares tras una videollamada con un «director financiero» creado mediante deepfake.*
<https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>

General de Protección de Datos (RGPD)⁶ se aplica en toda la Unión Europea desde mayo de 2018, estableciendo un marco común para la protección de los datos personales y la privacidad de las personas. El objetivo del RGPD es salvaguardar la privacidad de las personas y garantizar que las organizaciones que tratan datos personales rindan cuentas sobre cómo se recogen, almacenan y utilizan dichos datos.

Por ejemplo, si se filtra una copia escaneada del pasaporte de un huésped, la organización debe tomar medidas inmediatas para contener el incidente, evaluar el riesgo para las personas afectadas y, cuando sea necesario, notificarlo a la autoridad competente y a las personas afectadas. Una actuación tardía o incompleta puede agravar el perjuicio causado a los huéspedes y acarrear consecuencias normativas.

NIS2 y la resiliencia digital en la cadena de suministro

La Directiva NIS2⁷ es un marco de la UE que refuerza la seguridad y la resiliencia de los servicios y redes digitales. Exige a las organizaciones y a los proveedores de servicios críticos que gestionen los riesgos digitales, garanticen la continuidad del servicio y notifiquen los incidentes que perturben significativamente las operaciones o afecten a los socios conectados.

Mientras que el RGPD se centra en los datos personales, **la Directiva NIS2** aborda la **resiliencia y la continuidad de los servicios digitales**. Impone mayores exigencias a las organizaciones y a los proveedores de servicios críticos para que gestionen los riesgos digitales y notifiquen los incidentes que interrumpan o amenacen la disponibilidad de los servicios.

Por ejemplo, una pasarela de pago comprometida que impida el procesamiento de tarjetas en varios hoteles demuestra por qué son esenciales la resiliencia y la notificación de incidentes por parte de los proveedores. Cuando un proveedor falla, el impacto puede extenderse rápidamente a las organizaciones conectadas.

⁶ Parlamento Europeo y Consejo de la Unión Europea. (2016). *Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

⁷ Parlamento Europeo y Consejo de la Unión Europea. (2022). *Directiva (UE) 2022/2555, de 14 de diciembre de 2022, relativa a medidas para un nivel común elevado de ciberseguridad en toda la Unión (Directiva NIS2)*. Diario Oficial de la Unión Europea. <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

La NIS2 refuerza los requisitos de gestión de riesgos y notificación de incidentes entre los proveedores críticos y los prestadores de servicios. Dado que las organizaciones turísticas dependen en gran medida de sistemas externos —como **los PMS, los CRS y las plataformas de pago**—, unos controles deficientes a nivel de proveedor pueden transmitir el riesgo a lo largo de toda la cadena de suministro. Un cumplimiento deficiente o las notificaciones tardías alargan el tiempo necesario para contener los incidentes y aumentan la probabilidad de que el asunto llegue a las autoridades reguladoras, lo que conlleva multas más elevadas, la obligación de hacer pública la información y una interrupción más amplia del servicio que afecte a socios y clientes.

La Agencia de Ciberseguridad de la Unión Europea (ENISA, 2025)⁸ ofrece orientación técnica detallada sobre la implementación de medidas de gestión de riesgos de ciberseguridad en el marco de la NIS2. La guía hace hincapié en la evaluación estructurada de riesgos, los procedimientos de detección y notificación de incidentes, los controles de seguridad de la cadena de suministro y los mecanismos de mejora continua, todos ellos directamente relevantes para los ecosistemas turísticos interconectados.

Medidas prácticas para reducir el riesgo normativo y operativo

Para reducir la exposición y mejorar el cumplimiento normativo, las organizaciones deben centrarse en medidas prácticas y coordinadas:

- minimizar la cantidad de datos personales recopilados y conservados;
- definir claramente las funciones y responsabilidades en los contratos con proveedores y socios;
- aplicar controles de acceso y cifrado cuando sea pertinente;
- asegurarse de que el personal comprenda cuándo y cómo notificar los incidentes;
- probar los procedimientos de respuesta ante incidentes y de comunicación con los proveedores clave.

Estas medidas reducen los tiempos de detección y respuesta, limitan el riesgo legal y ayudan a mantener la confianza de los clientes durante y después de los incidentes.

⁸ Agencia de Ciberseguridad de la Unión Europea (ENISA). (2025). *Orientaciones técnicas de aplicación sobre medidas de gestión de riesgos de ciberseguridad (Versión 1.0)*. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

01

Explica dos obligaciones del RGPD que el personal debe cumplir y por qué son importantes.

02

Nombra tres sistemas típicos que aumentan la exposición y describe una forma en que una filtración

03

Más allá: ¿Cómo puede un incumplimiento del RGPD agravar un incidente a lo largo de una cadena de

Ir más allá

Los incumplimientos del RGPD —como la notificación tardía de una violación de datos, los acuerdos con proveedores incompletos o un registro inadecuado de incidentes— reducen el margen de tiempo para una contención eficaz. Cuando se combinan con sistemas interconectados, estos incumplimientos pueden permitir que las amenazas se propaguen a los socios, desencadenar medidas coercitivas más severas y transformar una violación de datos local en una crisis que afecte a varias organizaciones y al ecosistema turístico en su conjunto. Esto ilustra cómo los incumplimientos normativos pueden amplificar tanto la magnitud como el impacto de los incidentes digitales más allá de la organización directamente afectada.

Reflexión y debate

6. Funciones, responsabilidades y escalado

Unas funciones claras y una escalación oportuna son esenciales cuando se produce un incidente digital. Tan pronto como se detecte un problema, debe comunicarse inmediatamente a la persona de contacto designada. Este primer paso es fundamental, ya que la notificación temprana preserva las pruebas y desencadena una respuesta coordinada, en lugar de acciones aisladas o improvisadas.

En la mayoría de las organizaciones, la respuesta ante incidentes implica varias funciones definidas:

- **la persona que notifica el incidente**, que detecta y comunica el problema;
- un **primer interviniente** (a menudo personal de TI o de seguridad), que confirma que se ha producido un incidente;
- un **gestor de incidentes**, que coordina las decisiones y las actividades de respuesta;

- **los equipos de TI o de seguridad**, que llevan a cabo la contención técnica y la recuperación;
- **el equipo de comunicaciones**, que gestiona los mensajes internos y externos dirigidos a las partes interesadas;
- **el departamento jurídico o de cumplimiento normativo**, que evalúa las obligaciones reglamentarias, contractuales y de notificación.

Cada función se centra en una responsabilidad específica, lo que garantiza que los riesgos técnicos, jurídicos y de reputación se aborden de forma paralela y se gestionen correctamente.

Normas internacionales como la ISO/IEC 27001:2022⁹ hacen hincapié en la importancia de contar con funciones claramente definidas, procedimientos documentados y una respuesta estructurada ante incidentes como parte de un Sistema de Gestión de la Seguridad de la Información (SGSI). Estos principios refuerzan la necesidad de rendir cuentas y de una escalación controlada dentro de las organizaciones turísticas.

La importancia de la documentación

Es fundamental contar con una documentación exhaustiva en cada fase de un incidente. Registrar **lo que ocurrió, cuándo se tomaron las medidas y quién aprobó las decisiones** crea un registro de auditoría fiable. Esto facilita las investigaciones, la presentación de informes reglamentarios y el aprendizaje tras el incidente. Una buena documentación también acorta el tiempo de recuperación, ya que permite a los equipos ver qué medidas fueron eficaces y evitar repetir errores. Y lo que es más importante, protege tanto al personal como a la organización si las decisiones son revisadas posteriormente por la dirección, los organismos reguladores o los socios.

Por qué los incidentes no deben resolverse de forma individual

Los empleados no deben intentar resolver los incidentes digitales por su cuenta. Actuar de forma independiente puede destruir pruebas forenses, ampliar involuntariamente el alcance de una violación de seguridad o provocar una pérdida

⁹ Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. <https://www.iso.org/standard/27001>

adicional de datos. En su lugar, el personal debe seguir las instrucciones del responsable de incidentes o del equipo de TI/seguridad, lo que permite una contención controlada y los pasos correctos de notificación.

Es importante reconocer que los incidentes digitales afectan a personas reales y a puestos de trabajo reales. Los clientes pueden sufrir perjuicios, la carga de trabajo del personal aumenta durante los incidentes y las consecuencias para la organización se agravan cuando la escalación se retrasa o se gestiona de forma inadecuada.

Más allá

Los modelos de responsabilidad sencillos, como la **matriz RACI**, ayudan a aclarar las funciones en situaciones de presión al definir quién hace qué durante un incidente. En un modelo RACI:

- **«Responsable»** se refiere a la persona o equipo que lleva a cabo la tarea;
- **«Responsable»** es la persona que asume la responsabilidad final y aprueba las decisiones;
- **«Consultado»** incluye a quienes aportan ideas o conocimientos especializados;
- **«Informado»** incluye a quienes se mantienen al corriente de los avances.

En lo que respecta a la detección de incidentes, el miembro del personal que detecta y notifica el problema es el responsable, mientras que el gestor del incidente es el encargado de rendir cuentas. En cuanto a la contención de incidentes, los equipos de TI o de seguridad son los responsables, y el gestor del incidente sigue siendo el encargado de rendir cuentas, tras consultar a los equipos de apoyo pertinentes e informar a las partes interesadas clave.

Este enfoque estructurado reduce la confusión, evita la duplicación de esfuerzos y agiliza la toma de decisiones durante los plazos de respuesta limitados.

Reflexión y debate

01

¿Por qué deben los empleados evitar intentar resolver los incidentes digitales por su cuenta?

02

Menciona dos razones por las que la documentación es importante durante un incidente.

03

Más allá: en el ejemplo de RACI anterior, ¿quién es responsable de la contención y quién debe rendir cuentas?

Respuesta ante incidentes para pequeñas empresas turísticas

Muchas empresas turísticas son organizaciones pequeñas en las que el propietario, el gerente o unos pocos empleados desempeñan múltiples funciones. A menudo no se dispone de equipos especializados en ciberseguridad, lo que significa que los procedimientos de respuesta ante incidentes deben ser prácticos y fáciles de seguir.

Un modelo de respuesta sencillo puede ayudar a las organizaciones a reaccionar rápidamente cuando se produce un incidente cibernético:

1. Detectar

Reconocer actividades sospechosas o comportamientos inusuales

2. Contener

Limitar el impacto aislando los dispositivos, cuentas o sistemas afectados siempre que sea posible.

3. Notificar

Informar a la persona adecuada, al servicio de asistencia informática externo, al proveedor de servicios o a la autoridad competente.

4. Recuperar

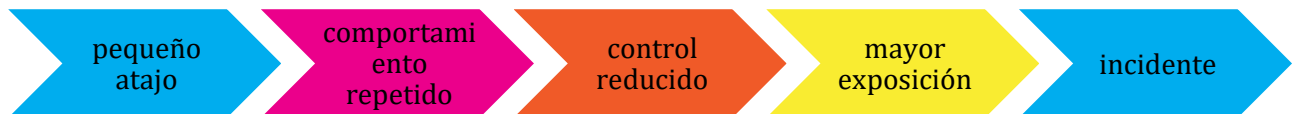
Restablecer el funcionamiento normal e identificar las lecciones que puedan ayudar a prevenir incidentes similares en el futuro.

Incluso las organizaciones pequeñas pueden responder de forma eficaz si el personal sabe qué hacer y a quién dirigirse. Unos procedimientos sencillos, la notificación oportuna y unas responsabilidades claras suelen ser más importantes que las soluciones técnicas complejas.

7. La seguridad digital en las operaciones turísticas cotidianas

La seguridad digital **solo** resulta eficaz **cuando se integra en el comportamiento operativo cotidiano**. Los conceptos presentados a lo largo de esta unidad —entre ellos, la ciberhigiene, la concienciación sobre los riesgos de la ingeniería social, la comunicación segura y el tratamiento responsable de los datos de los clientes— son fundamentales en las situaciones laborales cotidianas. Los incidentes digitales rara vez comienzan con ataques sofisticados. Lo más habitual es que **surjan de pequeños atajos operativos** que se toman durante los periodos de mayor actividad, cuando **el personal está bajo presión, centrado en la rapidez o gestionando múltiples solicitudes**. Aunque estas acciones puedan parecer insignificantes, las decisiones cotidianas influyen directamente en el riesgo digital.

El patrón de causa y efecto es sencillo:



Puede que un atajo aislado no cause ningún daño. Pero los atajos repetidos debilitan las barreras de protección. Con el tiempo, esto crea **vulnerabilidades estructurales** que los atacantes pueden aprovechar.

Cómo las decisiones cotidianas aumentan el riesgo

Entre los comportamientos operativos habituales que aumentan la exposición se incluyen:

- Reutilizar las credenciales de inicio de sesión «solo por hoy»
- Retrasar las actualizaciones del sistema porque el equipo de operaciones está muy ocupado
- Compartir el acceso para agilizar los procesos
- Ignorar mensajes de advertencia menores
- Aplazar la notificación de incidentes

Por separado, estas acciones parecen insignificantes. Sin embargo, si se repiten con el tiempo, reducen **la responsabilidad, la trazabilidad y la integridad del**

sistema. Esto aumenta la probabilidad de que **se produzcan fugas de datos, fraudes o interrupciones del servicio.**

Es importante ser consciente de ello: la eficiencia operativa y la seguridad digital deben complementarse, no competir entre sí.

Situaciones típicas de «zona gris»

Las zonas grises son situaciones en las que el personal debe elegir entre la rapidez y el cumplimiento estricto de los procedimientos. No se trata de infracciones intencionadas, sino de momentos en los que hay que tomar una decisión.

Ejemplo 1: inicio de sesión compartido durante un periodo de mucha actividad

Un miembro del personal mantiene la sesión de un sistema abierta para evitar tener que autenticarse repetidamente.

Riesgo: acceso sin supervisión, acciones no autorizadas, uso indebido de datos.

Ejemplo 2: Compartir credenciales de forma temporal

Se comparte el acceso para ayudar a un compañero a empezar a trabajar rápidamente.

Riesgo: pérdida de trazabilidad, incumplimiento normativo, imposibilidad de investigar incidentes.

Ejemplo 3: Notificación tardía

Aparece un mensaje inusual del sistema cerca del final del turno y no se notifica de inmediato. Riesgo: contención retrasada, agravamiento de los daños técnicos.

En cada caso, el objetivo inmediato es la comodidad. El resultado a largo plazo puede ser **una mayor exposición y un menor control.**

Por qué las pequeñas desviaciones conducen a incidentes

Cuando se repiten atajos poco seguros, se convierten en un comportamiento habitual. Con el tiempo, el personal puede dejar de reconocer el riesgo.

Ejemplo de progresión:

- Compartir la contraseña «solo por esta vez»
- Compartir de forma repetida
- Varias personas utilizan una misma cuenta
- Falta de responsabilidades claras
- Dificultad para investigar tras una filtración

Los incidentes digitales suelen producirse cuando se dan simultáneamente varias pequeñas vulnerabilidades.

He aquí el motivo:

- Es importante que las funciones estén bien definidas
- La coherencia en la presentación de informes es importante
- Los hábitos de ciberhigiene son importantes

Una seguridad digital sólida se construye a través de la disciplina diaria, no solo mediante herramientas técnicas. La seguridad digital refleja la interacción entre los controles técnicos y la disciplina conductual. Cuando las rutinas diarias ignoran pequeñas normas, la organización pierde poco a poco el control sobre quién puede acceder a los datos, modificar la información o detectar problemas de forma temprana. Esto reduce **la visibilidad, la rendición de cuentas y la rapidez de respuesta**. A medida que disminuye el control, aumenta la probabilidad de que **se produzcan filtraciones de datos, pérdidas económicas, consecuencias legales y daños a la reputación**. Por lo tanto, la disciplina diaria protege tanto a la organización como a las personas que dependen de sus sistemas.

Más allá

Los pequeños atajos operativos no solo aumentan el riesgo técnico, sino que revelan debilidades en **la cultura de riesgo y en los sistemas de control**. Cuando las decisiones en zonas grises son frecuentes, esto puede indicar una responsabilidad poco clara, una supervisión insuficiente o presiones de rendimiento desalineadas (por ejemplo, se premia más la rapidez que la seguridad).

El análisis avanzado se centra en identificar:

- Dónde se producen con mayor frecuencia los atajos

Unidad formativa 2: Seguridad digital en el Turismo

- Por qué el personal siente la presión de eludir los controles
Qué barreras fallaron (técnicas, de procedimiento o de gestión)
- Cómo se combinaron múltiples debilidades menores para dar lugar a un incidente

En lugar de preguntarse «¿Quién cometió el error?», la gestión avanzada de riesgos se pregunta:

¿Qué nivel de control ha fallado y cómo se puede reforzar el sistema?

Por lo tanto, mejorar la resiliencia digital requiere ambas cosas:

- Medidas de protección técnicas
- Una alineación organizativa entre las expectativas de eficiencia y seguridad

Reflexión y debate

01

¿Por qué los pequeños atajos operativos pueden aumentar el riesgo digital con el tiempo?

02

¿Qué es una situación de «zona gris» en materia de seguridad digital?

03

¿Por qué es importante analizar los fallos de control en lugar de centrarse únicamente en los errores individuales?

Recursos de vídeo complementarios

Simplilearn (2023) ofrece un recurso introductorio complementario que proporciona una visión general de los conceptos de ciberseguridad y los tipos de amenazas.

Canal: Simplilearn

Año: 2023

Título: ¿Qué es la ciberseguridad? | ¿Cómo funciona?

YouTube: <https://www.youtube.com/watch?v=inWWhr5tnEA>

8. Comprobación de conocimientos y ejercicios

Cuestionario de concienciación sobre seguridad digital

Objetivo: Evaluar la comprensión de los conceptos básicos de ciberseguridad, las prácticas de ciberhigiene y los fundamentos normativos.

Formato: Evaluación individual

Duración estimada: 20-30 minutos

Preguntas:

1. ¿Por qué se considera el turismo un sector de alto riesgo para la seguridad digital?
 - A. El turismo utiliza más sistemas en la nube que otros sectores.
 - B. El turismo depende de un elevado volumen de transacciones y de sistemas digitales interconectados.
 - C. Las empresas turísticas no forman a su personal en materia de tecnologías de la información.
 - D. El turismo gestiona pocos datos personales.

Respuesta correcta: B

2. ¿Cuál de las siguientes opciones describe mejor una vulnerabilidad?
 - A. Un tipo de malware.
 - B. Una debilidad que puede ser aprovechada por una amenaza.
 - C. Un requisito normativo.
 - D. Un incidente de seguridad.

Respuesta correcta: B

3. ¿Qué medidas reducen el riesgo de apropiación de cuentas? (Selecciona DOS respuestas)
 - A. Habilitar la autenticación multifactorial (MFA).

Unidad formativa 2: Seguridad digital en el Turismo

- B. Compartir contraseñas durante la temporada alta para agilizar el trabajo.
- C. Utilizar contraseñas seguras y únicas.
- D. Dejar las sesiones abiertas para agilizar los cambios de turno.

Respuesta correcta: A, C

4. Un miembro del personal recibe un correo electrónico urgente en el que un proveedor conocido solicita cambios inmediatos en los datos de pago. ¿Cuál es la medida más segura?
- A. Actualizar los datos de pago inmediatamente para evitar la interrupción del servicio.
 - B. Reenviar el correo electrónico a los compañeros para que lo confirmen.
 - C. Verificar la solicitud a través de un canal independiente (por ejemplo, llamando a un número conocido).
 - D. Ignorar el mensaje.

Respuesta correcta: C

5. Según el RGPD, las organizaciones deben (selecciona TRES respuestas):
- A. Proteger los datos personales mediante controles adecuados.
 - B. Notificar a las autoridades cuando sea necesario en caso de una violación de datos.
 - C. Almacenar todos los datos de los clientes de forma indefinida.
 - D. Limitar la recogida de datos a lo estrictamente necesario.

Respuesta correcta: A, B, D

6. ¿Cuál es el objetivo principal de la Directiva NIS2?
- A. Eliminar todos los incidentes cibernéticos.
 - B. Reforzar la resiliencia de los servicios digitales y la notificación de incidentes.

- C. Regular los precios del turismo.
- D. Aumentar la externalización de los servicios informáticos.

Respuesta correcta: B

7. ¿Por qué son arriesgadas las cuentas compartidas en los lugares de trabajo del sector turístico?
- A. Mejoran la rapidez operativa.
 - B. Reducen la rendición de cuentas y la trazabilidad.
 - C. Facilitan la investigación de incidentes.
 - D. Simplifican la presentación de informes de cumplimiento normativo.

Respuesta correcta: B

8. ¿Qué situación representa una decisión de «zona gris»?
- A. Bloquear el ordenador al levantarse del puesto de trabajo.
 - B. Negarse a compartir las credenciales de inicio de sesión bajo presión.
 - C. Dejar un sistema con sesión abierta durante la temporada alta para evitar tener que autenticarse repetidamente.
 - D. Informar inmediatamente de cualquier actividad sospechosa.

Respuesta correcta: C

9. ¿Por qué deben los empleados evitar resolver los incidentes digitales por su cuenta? (Selecciona DOS respuestas)
- A. Podría destruir pruebas o agravar la brecha de seguridad.
 - B. Demuestra iniciativa.
 - C. Garantiza una resolución más rápida.
 - D. Puede infringir los procedimientos internos de escalado.

Respuesta correcta: A, D

10. En un modelo RACI durante la contención de un incidente, ¿quién suele ser el responsable?
- A. El técnico de TI que realiza la reparación.
 - B. El gestor de incidentes que coordina la respuesta.
 - C. El miembro del personal que notificó el problema.
 - D. El cliente afectado por el incidente.

Respuesta correcta: B

11. ¿Por qué los pequeños atajos operativos se acumulan y acaban convirtiéndose en incidentes?
- A. Aumentan la velocidad del sistema.
 - B. Con el tiempo, normalizan los comportamientos poco seguros.
 - C. Activan automáticamente las alertas.
 - D. Eliminan la necesidad de informar.

Respuesta correcta: B

12. ¿Qué comportamiento favorece mejor la resiliencia digital en el turismo?
- A. Ignorar los mensajes de advertencia menores durante los periodos de mayor actividad.
 - B. Notificar inmediatamente cualquier actividad inusual a través de los canales establecidos.
 - C. Compartir el acceso al sistema con compañeros de confianza.
 - D. Aplazar las actualizaciones hasta el final de la temporada.

Respuesta correcta: B

13. ¿Por qué la respuesta ante una posible filtración de datos debe seguir los procedimientos establecidos en lugar de basarse en decisiones informales?

Unidad formativa 2: Seguridad digital en el Turismo

- A. Para evitar la destrucción de pruebas y garantizar el cumplimiento normativo.
- B. Para reducir la carga de trabajo de la dirección.
- C. Porque solo los socios externos son responsables.
- D. Porque los incidentes digitales se resuelven automáticamente si se ignoran.

Respuesta correcta: A

Ejercicio 1: Identificación de señales de alerta de phishing

Objetivo: Reforzar la capacidad de detectar intentos de phishing e ingeniería social en entornos de comunicación turística.

Formato: Debate en grupo o análisis en plenaria.

Duración estimada: 20-25 minutos.

Los participantes analizan un correo electrónico sospechoso simulado e identifican los indicadores de un posible fraude.

De: Servicio de asistencia para reservas <support@booking-example.com>

Para: Recepción del hotel

Asunto: URGENTE: Actualización de los datos bancarios para los próximos pagos

Estimado equipo del hotel:

Por favor, actualicen urgentemente la cuenta bancaria para los próximos pagos de los huéspedes. Se adjunta la última factura.

Si no se actualizan, los pagos podrían retrasarse.

Gracias,

Equipo de atención al cliente de Booking

Archivo adjunto: Invoice_0723.pdf

Señales de alerta a tener en cuenta (debate):

- 🚩 Lenguaje que denota urgencia o presión
- 🚩 Archivo adjunto inesperado
- 🚩 Saludo genérico («Equipo del hotel»)
- 🚩 Dominio del remitente ligeramente diferente o desconocido

Ejercicio 2: Clasificación para la priorización de riesgos digitales

Objetivo: Desarrollar un criterio estructurado para evaluar los riesgos digitales operativos.

Formato: Actividad en grupos reducidos.

Duración estimada: 25-30 minutos.

Los participantes clasifican los comportamientos enumerados según: a) la probabilidad de que se produzcan, b) el impacto potencial en caso de que se aprovechen y c) la prioridad de escalado. Los participantes deben proporcionar una breve justificación por escrito (2-3 frases) de sus decisiones de clasificación, explicando cómo interactúan la probabilidad y el impacto y por qué ciertos comportamientos requieren un mayor nivel de escalado.

Comportamientos que deben clasificarse por gravedad o probabilidad:

- ❖ Dejar sesiones abiertas en ordenadores compartidos
- ❖ Utilizar contraseñas débiles o repetidas
- ❖ Compartir credenciales con compañeros de trabajo
- ❖ Hacer clic en enlaces de remitentes desconocidos
- ❖ Ignorar las alertas del sistema o del software
- ❖ Aplazar las actualizaciones de software
- ❖ Conectar dispositivos personales a los sistemas de la empresa sin autorización
- ❖ Reenviar correos electrónicos con información confidencial

Ejercicio 3: Aplicación del marco normativo

Objetivo: Garantizar la comprensión correcta de los marcos normativos clave y sus implicaciones operativas.

Formato: Ejercicio individual.

Duración estimada: 5-10 minutos.

Empareja cada marco normativo con su finalidad principal. A continuación, proporciona un ejemplo práctico del sector turístico en el que se aplique dicha normativa.

Términos	Objetivos
RGPD	Proteger los datos personales y garantizar el cumplimiento de la normativa sobre privacidad
Directiva NIS2	Reforzar la resiliencia de los servicios digitales y la notificación de incidentes
Ley de gobernanza de datos	Regular el uso y el intercambio responsables de datos entre organizaciones
Código Ético Mundial de la OMT	Fomentar las prácticas éticas y el turismo sostenible

Ejercicio 4 – Debate estructurado: Rapidez frente a seguridad

Afirmación para el debate: «Se debería permitir al personal saltarse los pasos de verificación durante la temporada alta para mantener la rapidez operativa».

Objetivo: Desarrollar el pensamiento crítico en relación con la disyuntiva entre la eficiencia operativa y la seguridad digital.

Formato: Debate estructurado (equipos a favor y en contra).

Duración estimada: 25-30 minutos.

Los equipos preparan argumentos que aborden:

- las presiones en materia de eficiencia operativa,
- la amplificación de los riesgos de seguridad,
- las implicaciones normativas,
- el impacto en los huéspedes, el personal y la reputación de la organización.

Concluye con una reflexión en grupo sobre el equilibrio entre rapidez y seguridad.

2.2 Seguridad en los procesos del turismo digital

Al finalizar esta subunidad, los alumnos serán capaces de seguir procedimientos seguros para las reservas y los pagos, gestionar los datos de los clientes de forma responsable, actuar correctamente ante una sospecha de filtración de datos y colaborar con los equipos de TI y de seguridad.

- Gestión segura de los datos de los clientes: protección de las reservas y los pagos en línea
- La cadena de bloques para los pagos y más allá de los pagos (trazabilidad, verificación de identidad, programas de fidelización)
- Protocolos de respuesta ante filtraciones de datos (funciones y responsabilidades en las primeras 24 horas)

Actividad práctica sugerida:

- Ejercicio basado en un escenario: actividad de pago sospechosa

1. Procesos del turismo digital y puntos de riesgo

Los procesos del turismo digital están integrados en casi todas las etapas de la interacción con los huéspedes. Desde el momento en que se realiza una reserva hasta después de que finalice la estancia, los datos de los clientes circulan por múltiples sistemas. Estos procesos están diseñados para garantizar la eficiencia y la calidad del servicio, pero cada interacción digital conlleva un riesgo potencial.

Se produce un punto de riesgo digital cada vez que se crean, introducen, modifican, almacenan, transmiten o consultan datos. Cuanto más complejo e interconectado es un proceso, con mayor frecuencia se transfieren los datos entre sistemas y usuarios. Cada transferencia aumenta la exposición tanto a errores accidentales como a un uso indebido intencionado.

La relación entre la complejidad del proceso y el riesgo sigue una lógica acumulativa:

- cuantos más sistemas intervengan → más puntos de integración;
- cuantos más usuarios intervengan, más credenciales de acceso habrá;
- más intercambios automatizados → más dependencias de configuración;
- más socios externos → mayor exposición de la cadena de suministro.

Dónde suelen aparecer los puntos de riesgo

Los puntos de riesgo en los procesos turísticos suelen darse en las siguientes situaciones operativas:

1. **Introducción de datos y gestión de reservas:** La introducción manual de datos en los sistemas PMS o CRS conlleva la posibilidad de errores, duplicaciones o divulgación accidental. Si los controles de autenticación son débiles, personas no autorizadas pueden acceder a los datos de las reservas.
2. **Procesamiento de pagos:** Las etapas de pago representan objetivos de gran valor, ya que implican datos financieros. Entre los riesgos se incluyen:
 - conexiones de pago inseguras;
 - patrones de transacciones inusuales;
 - información de facturación que no coincide;
 - fallos repetidos en las autorizaciones;
 - el fraude con tarjeta no presente.

Si no se detectan o notifican estas anomalías, pueden producirse pérdidas económicas y devoluciones de cargos.

3. **Transferencias entre sistemas:** Las integraciones automatizadas entre el PMS, el CRM, las plataformas de reservas y las pasarelas de pago mejoran la eficiencia, pero introducen riesgos de dependencia. Las configuraciones erróneas o las credenciales comprometidas en un sistema pueden propagarse a las plataformas conectadas.
4. **Gestión de accesos y cambios de turno:** Los cambios en los permisos de los usuarios, los terminales compartidos y las transiciones entre turnos crean momentos de menor responsabilidad. Los atajos temporales pueden debilitar la trazabilidad y complicar la investigación de incidentes.

Interacción entre el riesgo técnico y el riesgo humano

Los puntos de riesgo operativo reflejan la interacción entre las vulnerabilidades técnicas y el comportamiento humano. Una debilidad técnica, como una configuración insegura, puede permanecer latente hasta que se active por un error humano. A la inversa, un pequeño atajo humano puede dejar al descubierto una vulnerabilidad del sistema que, de otro modo, seguiría siendo inofensiva.

Por ejemplo:

- Una recepcionista reutiliza unas credenciales para agilizar el registro de entrada.
- Se utiliza una cuenta de correo electrónico comprometida para restablecer una contraseña.
- Un retraso en la actualización deja sin parchear una vulnerabilidad conocida.

Por separado, estas acciones pueden parecer insignificantes. Combinadas, pueden crear las condiciones para que se produzcan incidentes graves.

Higiene digital física

Los riesgos digitales en entornos turísticos no se limitan al software y a los flujos de datos. Muchos incidentes tienen su origen en **el acceso físico a los sistemas digitales**, especialmente en entornos operativos como las recepciones de los hoteles, las estaciones de trabajo compartidas o las zonas administrativas.

Los dispositivos desatendidos, un control deficiente del acceso físico o el uso de dispositivos externos pueden crear puntos de entrada para los atacantes. En entornos muy dinámicos, con múltiples turnos de personal e interacción con los huéspedes, estos riesgos se amplifican.

Algunos ejemplos típicos son:

- dejar desatendida una terminal de registro mientras se está conectado;
- permitir el acceso a las zonas administrativas o a las salas de servidores sin supervisión;
- conectar dispositivos USB desconocidos a ordenadores operativos;
- mostrar información confidencial en pantallas visibles para los huéspedes.

Incluso acciones tan sencillas como dejar abierta la puerta de una sala de servidores para ventilar pueden socavar unas medidas de seguridad digital que, por lo demás, serían sólidas.

Por este motivo, la higiene digital física debe considerarse parte del comportamiento operativo cotidiano, complementando los controles técnicos y reduciendo la probabilidad de que pequeños descuidos se conviertan en incidentes de mayor envergadura.

Priorización estructurada de riesgos en las operaciones turísticas

Unidad formativa 2: Seguridad digital en el Turismo

El riesgo digital en entornos turísticos no debe evaluarse de forma intuitiva, sino mediante una priorización estructurada. Dos dimensiones principales determinan la urgencia:

- Probabilidad (probabilidad de que se produzca)
- Impacto (operativo, financiero, normativo, reputacional)

Una tabla de evaluación simplificada permite dar una respuesta proporcional:

Impacto / Probabilidad	Bajo	Medio	Alto
Bajo impacto	Bajo	Bajo	Bajo
Impacto medio	Bajo	Medio	Medio
Alto impacto	Medio	Alto	Crítico

Los riesgos que combinan un impacto elevado y una probabilidad elevada requieren atención inmediata y medidas de mitigación. Los riesgos de menor prioridad deben seguir siendo objeto de seguimiento, pero es posible que no requieran el mismo nivel de recursos ni la misma urgencia.

El papel de los empleados en la gestión de los puntos de riesgo

Los empleados actúan tanto como usuarios como garantes de la seguridad en los procesos digitales. Su comportamiento influye directamente en que un punto de riesgo se agrave o no.

El personal debe:

- seguir los procedimientos definidos al introducir o modificar datos;
- verificar las solicitudes inusuales antes de actuar;
- estar atentos a patrones de transacciones irregulares;
- evitar compartir credenciales, ni siquiera de forma temporal;
- notificar inmediatamente cualquier sospecha de irregularidad a través de los canales establecidos.

Tal y como se destaca en la subunidad 2.1, la escalación temprana es fundamental para evitar que las irregularidades localizadas se conviertan en incidentes sistémicos. En contextos operativos como el procesamiento de pagos y la gestión de

reservas, el retraso en la notificación aumenta significativamente el riesgo financiero y normativo.

Los incidentes digitales en los procesos turísticos tienen consecuencias tangibles. Los huéspedes pueden sufrir pérdidas económicas o violaciones de la privacidad, y las organizaciones pueden enfrentarse a daños a su reputación u obligaciones normativas. La continuidad operativa depende de un comportamiento responsable en cada paso digital.

Más allá

La cartografía de riesgos a lo largo de todo el recorrido digital del cliente ofrece un método estructurado para analizar la exposición. En lugar de evaluar tareas aisladas, las organizaciones examinan:

- dónde se recopilan los datos;
- dónde se almacenan;
- dónde se transfieren entre sistemas;
- dónde se modifican los permisos;
- dónde intervienen proveedores externos.

El riesgo suele ser mayor en los puntos de transición, sobre todo cuando los datos cambian de titularidad o de control del sistema. Identificar estas etapas permite a las organizaciones dar prioridad a las medidas de control de mayor impacto, en lugar de distribuir los recursos de manera uniforme entre todos los pasos del proceso.

Actividad práctica: Identificación de puntos de riesgo en un proceso turístico real

Objetivo: Identificar los puntos de riesgo digital sistémico en un proceso turístico seleccionado.

Formato: Taller en grupos reducidos (3-4 participantes)

Duración estimada: 45-60 minutos

En pequeños grupos, elegid un proceso turístico común, por ejemplo:

- la gestión de una reserva en línea;
- la tramitación de un reembolso;
- gestionar reservas de grupo;
- actualizar la información de los huéspedes durante el registro de entrada;
- coordinarse con una plataforma de reservas externa.

Para el proceso seleccionado, identifica:

- Un punto de riesgo durante la introducción de datos.
- Un punto de riesgo durante la transferencia entre sistemas.
- Un riesgo relacionado con el comportamiento humano.
- Un momento en el que podría ser necesario escalar el problema o informar de él.

Para cada punto de riesgo identificado, describe brevemente:

- qué podría salir mal;
- cuál sería la consecuencia potencial;
- una medida preventiva.

Tras 10-15 minutos, cada grupo presenta sus conclusiones.

Reflexión y debate

01

¿Qué es un punto de riesgo digital y por qué aumentan los puntos de riesgo en los procesos digitales?

02

Da un ejemplo de riesgo durante el procesamiento de un pago y una acción correcta que debe realizar el empleado.

03

¿Por qué es más eficaz analizar el riesgo a lo largo de todo el recorrido del cliente que revisar cada paso por separado?

2. Gestión segura de los datos de los clientes

La gestión segura de los datos de los clientes es una **responsabilidad operativa fundamental** en las organizaciones turísticas. Los registros de reservas, los datos de identidad, la información de contacto y los datos relacionados con los pagos se procesan a diario a través de sistemas CRM y plataformas interconectadas. Estos sistemas permiten la eficiencia y la personalización del servicio, pero también concentran datos personales estructurados. Si los controles son deficientes, pueden convertirse en puntos de exposición de gran impacto.

Una protección de datos eficaz comienza con una recopilación selectiva. Las organizaciones deben recopilar únicamente la información necesaria para prestar el servicio y cumplir con las obligaciones legales. Recopilar campos adicionales por comodidad aumenta el volumen de datos sensibles almacenados y, por lo tanto, aumenta el impacto potencial en caso de que los sistemas se vean comprometidos.

Este principio, conocido como minimización de datos, reduce el riesgo en la práctica:

- menos elementos de datos sensibles almacenados;
- menor impacto de las violaciones de seguridad;
- supervisión y control simplificados;
- menor exposición en materia de cumplimiento normativo en caso de incidente.

Limitar la recogida de datos no es una restricción técnica, sino una decisión estratégica de gestión de riesgos.

El principio de minimización de datos se establece explícitamente en el artículo 5, apartado 1, letra c), del Reglamento General de Protección de Datos (RGPD), que exige que los datos personales sean «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se tratan» (Reglamento (UE) 2016/679)¹⁰.

Control de acceso y medidas de seguridad del sistema

Tras la recogida de datos, las medidas de seguridad operativas deben garantizar que solo el personal autorizado pueda acceder a la información de los clientes o tratarla.

¹⁰ Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos)*. Diario Oficial de la Unión Europea. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679>

Entre los controles fundamentales se incluyen:

- permisos de acceso basados en funciones y alineados con **los puestos de trabajo** (el acceso se concede en función de **los cargos** —por ejemplo, RR. HH., Finanzas— en lugar de a personas concretas, lo que garantiza que los usuarios solo vean las herramientas relevantes para su departamento específico);
- aplicación del principio del mínimo privilegio (a los usuarios se les conceden los niveles de acceso **mínimos** imprescindibles para realizar sus tareas, lo que limita estrictamente el daño potencial derivado de una cuenta comprometida);
- autenticación multifactorial (MFA) (requiere **dos o más pruebas** de identidad —por ejemplo, una contraseña más un código de teléfono— para iniciar sesión, lo que hace que las contraseñas robadas sean inútiles por sí solas);
- cifrado de datos sensibles tanto en reposo como en tránsito (codifica los datos en un código ilegible tanto mientras están **almacenados** en un disco como mientras se **transmiten** por Internet o por una red);
- registro y supervisión de accesos, exportaciones y modificaciones (crea un **registro digital** de quién ha consultado, modificado o trasladado datos, lo que permite a los equipos de seguridad detectar e investigar actividades sospechosas en tiempo real).

En entornos de CRM, la supervisión es especialmente importante. Indicadores como horas de inicio de sesión inusuales, exportaciones repetidas de datos, modificaciones masivas de registros o accesos desde ubicaciones inesperadas pueden indicar un uso indebido o una vulneración de la seguridad. La detección temprana limita significativamente la gravedad del problema.

La gestión segura de los accesos también requiere atención durante los cambios de personal, las transiciones entre turnos y las modificaciones de funciones. La retirada tardía de permisos o de credenciales compartidas debilita la trazabilidad y aumenta la exposición.

Comportamiento operativo y agravamiento de la situación

Las medidas de seguridad técnicas por sí solas no son suficientes. La gestión segura de los datos depende en igual medida de un comportamiento disciplinado por parte de los empleados.

El personal debe:

- evitar almacenar datos de pago en campos de texto libre o notas internas;
- evitar exportar datos a menos que sea necesario desde el punto de vista operativo;
- seguir los procedimientos formales para las correcciones y eliminaciones;
- cerrar la sesión en los sistemas cuando no se utilicen;
- cuestionar las solicitudes de acceso inusuales.

Tal y como se ha establecido en secciones anteriores, la adopción de medidas correctivas de forma independiente ante posibles incidentes puede destruir los registros de auditoría y complicar la evaluación regulatoria. La escalación a través de los canales definidos garantiza la conservación de las pruebas y la toma de decisiones coordinada.

La escalación oportuna permite al departamento de TI y a la dirección evaluar las medidas de contención y determinar si se aplican obligaciones de notificación. La actuación temprana reduce directamente las interrupciones operativas y el daño a la reputación.

Conservación, eliminación e integración segura

La seguridad de los datos va más allá del acceso y la supervisión. Conservar los datos más tiempo del necesario aumenta la exposición sin aportar ningún beneficio operativo. Unas políticas claras de conservación y eliminación deben definir:

- los períodos de conservación de los datos de reservas y reservas;
- la anonimización o tokenización de la información relacionada con los pagos;
- los procedimientos de autorización para la supresión;
- la documentación de las acciones de supresión.

La integración segura con las plataformas de pago es igualmente importante. Los sistemas CRM deben evitar almacenar los datos completos de las tarjetas, salvo que sea estrictamente necesario y se cumplan las normas de seguridad de los pagos. Siempre que sea posible, la tokenización o las pasarelas seguras reducen la concentración del riesgo financiero.

Las pruebas de los procedimientos de respuesta ante incidentes —incluida la cooperación con el departamento de TI y los proveedores externos— completan el ciclo de gestión segura de los datos. La detección, la contención, la documentación y la comunicación deben funcionar de forma conjunta.

En conjunto, estas medidas crean un marco estructurado de protección de datos: recogida controlada → acceso restringido → uso supervisado → retención definida → supresión documentada.

Actividad práctica: Ejercicio de revisión de riesgos del CRM

Los alumnos analizan una estructura simplificada de CRM que contiene: datos de contacto de los huéspedes, documentos de identidad escaneados, números completos de tarjetas de pago, notas internas, historial de marketing y datos de reservas archivados durante diez años.

1. Identifica qué elementos de datos representan el mayor riesgo.
2. Identifica qué elementos de datos pueden exceder la necesidad operativa.
3. Proponer una mejora en el control de acceso.
4. Proponer una mejora en la política de conservación de datos.
5. Explica qué cambio reduciría más el riesgo global y por qué.

Más allá

Una evaluación avanzada de la minimización de datos implica una revisión estructurada de:

- los campos de datos obligatorios frente a los opcionales;
- fuentes de datos automatizadas e integraciones externas;
- los plazos de conservación y la verificación de la supresión;
- prácticas de seudonimización o tokenización;
- la correspondencia entre las necesidades operativas y la información almacenada.

Dar prioridad a las correcciones en los casos en que los datos innecesarios se conservan durante más tiempo permite reducir al máximo la exposición.

Reflexión y debate

01

¿Qué es la minimización de datos y por qué constituye una medida estratégica de gestión de riesgos?

02

Nombra dos medidas de seguridad operativas que protejan los datos del CRM y explica cómo una de ellas reduce el impacto.

03

Más allá: ¿Cómo priorizarías las mejoras en un sistema CRM con un exceso de datos almacenados?

3. Pagos, fraude y estafas en las reservas

Los pagos y las reservas representan etapas de gran valor en los procesos del turismo digital, ya que implican directamente transacciones financieras y la confianza de los clientes. A diferencia de la exposición general de datos, los incidentes relacionados con los pagos suelen provocar un perjuicio inmediato y cuantificable: pérdidas económicas, devoluciones de cargos, daño a la reputación y un aumento de la carga de trabajo operativo.

El fraude en el turismo suele centrarse en los puntos en los que se mueve el dinero o en los que existen obligaciones de reembolso. La combinación de transacciones a distancia, la presión del tiempo y las reservas transfronterizas aumenta la vulnerabilidad.

Tipos comunes de fraude en el turismo

En las operaciones turísticas aparecen habitualmente varios patrones de fraude:

- **Fraude sin presencia de la tarjeta (CNP):** datos de tarjetas robadas que se utilizan sin verificar físicamente la tarjeta;
- **Cuentas robadas o comprometidas:** los atacantes acceden a perfiles de reserva y modifican las reservas;
- **Estafas en las reservas mediante identidades falsas:** se realizan reservas fraudulentas para manipular los precios o las políticas de cancelación;
- **Suplantación de identidad en el correo electrónico empresarial (BEC):** los atacantes se hacen pasar por proveedores o socios para desviar pagos;
- **Manipulación de reembolsos:** solicitudes de reembolso falsas que se aprovechan de la confusión operativa.

Los estafadores rara vez se basan únicamente en la sofisticación técnica. Muchos ataques se aprovechan de la urgencia, la confianza o los atajos en los procedimientos.

Señales de alerta e indicadores operativos

La detección eficaz del fraude depende del reconocimiento de patrones, más que de anomalías aisladas. Entre las señales de alerta típicas en los entornos de pago y reserva del sector turístico se incluyen:

- importes de reserva inusualmente elevados;
- varias reservas realizadas en rápida sucesión desde la misma cuenta o dirección IP;

- discrepancias entre la información de facturación y la de contacto;
- autorizaciones fallidas repetidas;
- solicitudes urgentes para modificar los datos de pago;
- presión para eludir los procedimientos normales de verificación.

Por sí solas, estas señales pueden reflejar irregularidades operativas más que un fraude confirmado. Sin embargo, su valor analítico aumenta significativamente cuando se evalúan de forma combinada.

Para facilitar una evaluación estructurada, los indicadores de fraude pueden clasificarse en tres niveles analíticos:

- **Anomalías aisladas:** una única transacción irregular o discrepancia sin indicios de un patrón
- **Anomalías de patrón:** irregularidades repetidas procedentes de la misma dirección IP, dispositivo, cuenta o método de pago
- **Señales de fraude coordinado:** indicadores compuestos, como reservas a gran velocidad combinadas con discrepancias de identidad y lenguaje que denota urgencia

Los indicadores de los niveles superiores requieren una escalación inmediata, ya que suelen indicar un fraude estructurado u organizado, más que irregularidades accidentales. Dar prioridad a los patrones compuestos mejora significativamente la eficiencia de la detección y reduce las interrupciones operativas innecesarias.

Respuesta operativa ante transacciones sospechosas

Cuando un pago o una reserva parezcan sospechosos, la actuación inmediata debe seguir procedimientos estructurados en lugar de basarse en un criterio informal.

El personal debe:

- suspender la tramitación de la transacción;
- evitar tramitar reembolsos o modificaciones sin verificación previa;
- solicitar una confirmación adicional a través de los canales autorizados;
- remitir el asunto a los departamentos de finanzas, informática o dirección, de acuerdo con los procedimientos establecidos;
- documentar las medidas adoptadas.

Intentar «resolver el problema rápidamente» bajo presión operativa puede aumentar el riesgo. Una escalación estructurada protege tanto a los clientes como a la organización.

Controles de prevención

La prevención del fraude combina medidas de seguridad técnicas y disciplina conductual.

Entre los controles clave se incluyen:

- **Pasarelas de pago seguras**, que garantizan un procesamiento cifrado y reducen la exposición de los datos de las tarjetas en los sistemas internos;
- **La autenticación 3-D Secure (3DS)**, que añade un paso de verificación adicional para confirmar la identidad del titular de la tarjeta durante las transacciones en línea;
- **Supervisión de transacciones y reglas de velocidad**, que detectan patrones inusuales, como reservas rápidas y repetidas, transacciones repentinas de alto valor o autorizaciones fallidas repetidas;
- **Separación de funciones en la aprobación de pagos**, en la que diferentes miembros del personal autorizan y procesan los movimientos financieros para reducir el riesgo de fraude interno y externo;
- **Umbral de escalación claros**, que definen cuándo una transacción debe ser revisada por la dirección o el departamento de TI en lugar de procesarse automáticamente;
- **Formación periódica sobre concienciación frente al fraude**, que refuerza el reconocimiento de tácticas de presión, intentos de suplantación de identidad y anomalías en las reservas.

Ningún control por sí solo es suficiente. Las medidas de seguridad por capas reducen tanto la probabilidad como el impacto.

Contexto normativo

La prevención del fraude en el procesamiento de pagos se ve reforzada por los requisitos normativos europeos. **La Directiva (UE) 2015/2366 sobre servicios de pago (PSD2)**¹¹ introdujo la obligación de la autenticación fuerte del cliente (SCA) para los pagos electrónicos. La SCA requiere al menos dos factores de autenticación independientes y suele implementarse mediante mecanismos como 3-D Secure (3DS).

¹¹ Unión Europea. (2015). *Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior (PSD2)*. Diario Oficial de la Unión Europea.
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366>

Para las organizaciones turísticas, esto significa que la verificación segura de los pagos no es simplemente una buena práctica, sino que forma parte de un marco normativo destinado a reducir el fraude en línea y a proteger a los consumidores dentro de la Unión Europea.

Escenario

El incidente: Llega un correo electrónico de un proveedor con el que se lleva trabajando mucho tiempo en el que se indica que su cuenta bancaria ha cambiado y se solicita una actualización urgente de los datos de pago. El mensaje insiste en que, si no se actualiza de inmediato, podría producirse una interrupción del servicio para un evento próximo.

«¡Si no actualizas esto ahora, no entregaremos la comida para el banquete de boda de esta noche!»

Tarea en grupo

1. Indicadores de alerta en el mensaje.
2. Riesgos si se tramita la solicitud sin verificarla.
3. Pasos correctos de verificación.
4. Procedimientos de escalado necesarios.
5. ¿Qué control podría haber evitado o limitado el riesgo?

Más allá

El análisis de patrones de fraude consiste en identificar qué indicadores predicen con mayor certeza los ataques organizados o automatizados. Las reservas a gran velocidad, las transacciones repentinas de alto valor, los fallos repetidos en las autorizaciones y las inconsistencias en las direcciones IP o los dispositivos suelen indicar una actividad fraudulenta estructurada.

Dar prioridad a la supervisión de estos indicadores de alto impacto mejora la eficacia de la detección y reduce las fricciones operativas innecesarias.

Reflexión y debate

01

Nombra dos tipos comunes de fraude en los pagos en el sector turístico y un indicador para cada uno.

02

¿Cuál es la respuesta inmediata correcta cuando una transacción parece sospechosa?

03

¿Por qué la presión operativa puede aumentar el riesgo de fraude?

04

Más allá: ¿Qué indicadores de fraude deben priorizarse en los sistemas de supervisión y por qué?

4. Ejercicio de simulación: pago sospechoso

Actividad práctica

Objetivo: Aplicar la jerarquía de detección de fraudes y los procedimientos estructurados de escalado.

Formato: Análisis en grupo basado en un escenario

Duración estimada: 30-40 minutos

Descripción del escenario:

Un miembro del departamento de contabilidad recibe un correo electrónico de un proveedor habitual (por ejemplo, un servicio de lavandería o un distribuidor de alimentos). La solicitud parece verosímil. La relación con el proveedor es auténtica y la fecha coincide con el pago programado.

El mensaje dice lo siguiente:

«Estimado departamento de contabilidad: a continuación les facilitamos los datos bancarios actualizados para nuestra próxima factura mensual. Nuestra cuenta anterior va a ser cerrada debido a una auditoría. Les rogamos que actualicen sus registros de inmediato y confirmen cuándo está previsto el pago de la próxima semana. Si no se actualizan los datos, podría producirse una suspensión del servicio».

Archivo adjunto: [Nuevos_datos_bancarios_y_factura.pdf](#)

Debate en grupo: ¿Cómo reaccionar?

Los alumnos analizan el escenario en pequeños grupos, centrándose en tres etapas estructuradas de evaluación: identificar el punto de riesgo, reconocer los indicadores de alerta y definir la respuesta operativa correcta.

Paso 1: Identificar el punto de riesgo

Debate:

- ¿Por qué el departamento de contabilidad es un objetivo de gran valor?
- ¿Qué autoridad operativa hace que este departamento sea especialmente vulnerable?

Aspecto clave:

Los equipos de contabilidad tienen autoridad directa para modificar registros de pago y realizar transferencias financieras. Una brecha de seguridad en este punto provoca un perjuicio financiero inmediato, en lugar de consecuencias diferidas o indirectas.

Paso 2: Identificación de indicadores de alerta

Los alumnos identifican posibles señales de alerta, tales como:

- un lenguaje que denota urgencia y presión;
- solicitud de modificación de los datos de pago establecidos;
- amenazas de interrupción del servicio;
- explicación inesperada del cierre de la cuenta;
- un archivo adjunto en el que se solicita una acción.

Aunque es posible que el correo electrónico no contenga enlaces maliciosos, el riesgo radica en la manipulación de los procedimientos más que en el malware.

Este escenario refleja un tipo de fraude habitual: el «**Business Email Compromise**» (BEC).

Paso 3: Respuesta estructurada

Los alumnos determinan la secuencia de respuesta correcta.

Las medidas adecuadas incluyen:

- suspender la modificación del pago;
- abstenerse de actualizar los datos bancarios de inmediato;
- verificar la solicitud a través de un canal independiente (por ejemplo, llamando al proveedor utilizando un número de contacto verificado ya existente);
- remitir el asunto a un nivel superior dentro de la empresa, de acuerdo con los procedimientos de control financiero;
- documentar la interacción.

La verificación debe realizarse a través de un canal de comunicación independiente. El uso de la información de contacto facilitada en el correo electrónico sospechoso no constituye una verificación independiente.

Los alumnos también deben tener en cuenta:

- en qué momento se debe informar a la dirección o al departamento de TI;
- cómo la documentación protege tanto al empleado como a la organización;
- qué control existente (por ejemplo, la separación de funciones) debería evitar esta situación.

5. Las primeras 24 horas tras una filtración de datos

Cuando se detecta una **filtración de datos**, las primeras 24 horas son cruciales. Las decisiones tempranas influyen en la magnitud del impacto, la exposición a las normas reguladoras, la interrupción de las operaciones y el daño a la reputación. Los retrasos o las acciones descoordinadas durante este periodo pueden aumentar significativamente el perjuicio.

La prioridad inmediata es **la contención**. La contención implica aislar los sistemas afectados, detener el acceso no autorizado y evitar que la filtración se extienda aún más. Si se retrasa la contención, pueden quedar expuestos más datos, la

recuperación del sistema se vuelve más compleja y aumentan los costes económicos y de reputación.

Sin embargo, la contención debe llevarse a cabo de forma controlada y documentada.

Prioridades inmediatas en las primeras 24 horas

La respuesta inicial debe centrarse en las siguientes acciones: identificar los sistemas afectados y las categorías de datos, aislar las cuentas o sistemas comprometidos, conservar los registros y las pruebas, notificar a los contactos internos de escalación y documentar todas las medidas adoptadas. La conservación de las pruebas es especialmente importante. Los intentos descoordinados de «limpiar» los sistemas pueden destruir rastros forenses, lo que dificulta la investigación y puede aumentar el riesgo normativo.

Como se ha destacado anteriormente, una intervención descoordinada puede ampliar involuntariamente el alcance de la violación de seguridad o comprometer las pruebas forenses. En las primeras 24 horas, una escalación disciplinada y una contención controlada son esenciales para limitar la exposición normativa y reputacional.

Documentación y registro de auditoría

Es esencial llevar a cabo una documentación precisa durante las primeras 24 horas. Se debe registrar en una cronología clara:

- **cuándo** se detectó la violación;
- **quién** la notificó;
- **qué sistemas** se vieron afectados;
- **qué medidas de contención** se adoptaron;
- **quién** autorizó las decisiones.

Este registro de auditoría sirve de apoyo para la investigación, la presentación de informes reglamentarios y el aprendizaje tras el incidente. Además, protege a los empleados al demostrar que se siguieron los procedimientos.

FIRST 24 HOURS AFTER A DATA BREACH

Critical actions to limit impact, protect individuals and ensure compliance

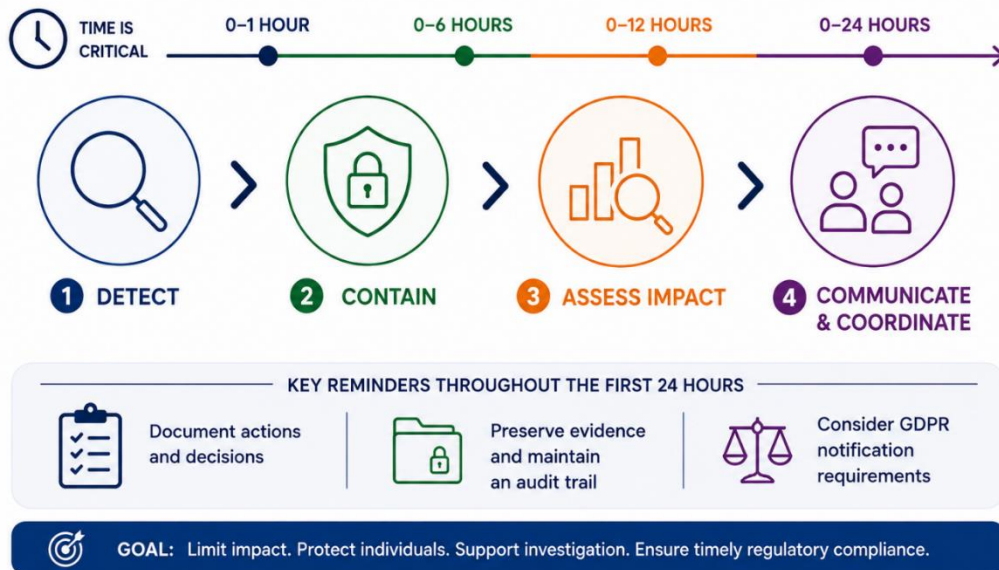


Figura 3: Fases clave de la respuesta durante las primeras 24 horas tras una filtración de datos

Consideraciones normativas

De conformidad con el artículo 33, apartado 1, del Reglamento General de Protección de Datos (RGPD, 2016), las organizaciones deben notificar a la autoridad de control competente en un plazo de 72 horas desde que tengan conocimiento de una violación de datos personales, salvo que sea improbable que dicha violación suponga un riesgo para las personas físicas.

«En caso de violación de datos personales, el responsable del tratamiento notificará sin demora injustificada y, cuando sea factible, a más tardar 72 horas después de haber tenido conocimiento de ella, la violación de datos personales a la autoridad de control (...) salvo que sea improbable que la violación de datos personales suponga un riesgo para los derechos y libertades de las personas físicas.» (RGPD, 2016, art. 33)

Además, el artículo 34 exige a las organizaciones que **comuniquen la violación directamente a las personas afectadas** cuando sea probable que suponga un riesgo elevado para sus derechos y libertades.

Esto significa que, durante las primeras 24 horas, las organizaciones no solo deben contener la violación, sino también llevar a cabo una **evaluación preliminar**

estructurada del impacto para determinar las consecuencias normativas y operativas. En concreto, deben evaluar:

- si hay datos personales implicados;
- el nivel de riesgo para las personas afectadas;
- si es necesario notificarlo a la autoridad de control;
- si puede ser necesaria la comunicación directa a las personas afectadas.

Una evaluación temprana y estructurada reduce tanto el riesgo normativo como el daño a la reputación.

Para respaldar esta evaluación, las organizaciones deben aplicar un marco de puntuación rápida del impacto basado en criterios definidos:

1. Sensibilidad de los datos implicados (identidad, pagos, salud, hábitos de viaje)
2. Volumen de registros potencialmente afectados
3. Importancia crítica de los sistemas afectados (operaciones principales frente a sistemas auxiliares)
4. Posible exposición normativa

La aplicación de una escala de puntuación sencilla de 1 a 3 por categoría permite establecer prioridades justificables, respalda la adopción de medidas de contención proporcionadas y refuerza la base jurídica para las decisiones de notificación a las autoridades de control dentro del plazo de 72 horas establecido por el RGPD.

Comunicación y reputación

Durante el primer día, las organizaciones deben preparar **planes de comunicación internos y externos claros**. La comunicación debe ser precisa, objetiva y coordinada. Las declaraciones prematuras o especulativas pueden aumentar la confusión y el daño a la reputación.

Los incidentes digitales afectan a los clientes, a la carga de trabajo del personal y a la estabilidad de la organización. Ser consciente de estas repercusiones más amplias refuerza la necesidad de una actuación estructurada y oportuna.

Escenario: Planificación de la respuesta en 24 horas

Un miembro del personal informa de que un usuario no autorizado ha accedido al sistema de reservas durante la noche. Es posible que se hayan consultado o exportado varios registros de huéspedes.

En pequeños grupos, los alumnos:

- Definirán las tres primeras medidas que deben adoptarse.
- Identificarán a qué responsables hay que informar.
- Determinarán si puede ser necesaria una notificación a las autoridades reguladoras.
- Describan qué debe documentarse en las primeras 24 horas.

Los grupos justifican sus decisiones basándose en el impacto y el riesgo.

Más allá

Responder con rapidez es esencial, pero actuar sin una estructura definida puede aumentar la exposición al riesgo. Las acciones precipitadas pueden pasar por alto obligaciones legales o destruir pruebas. Por el contrario, una cautela excesiva puede permitir que la infracción se extienda.

Una respuesta eficaz equilibra la rapidez con un procedimiento estructurado. Unas vías de escalación claras, unas funciones predefinidas y una toma de decisiones documentada permiten a las organizaciones actuar con rapidez al tiempo que cumplen los requisitos normativos y operativos.

Reflexión y debate

01

¿Cuál es la principal prioridad durante las primeras 24 horas tras una filtración de datos, y por qué?

02

¿Por qué deben los empleados notificar los incidentes de inmediato en lugar de intentar solucionarlos por su cuenta?

03

¿Qué información debe documentarse durante la fase de respuesta inicial?

6. Cooperación con los equipos de TI y los proveedores externos

Una cooperación eficaz con los equipos de TI y los proveedores externos es esencial en entornos turísticos interconectados digitalmente. Las reservas, los pagos, los sistemas CRM, los servicios en la nube y las plataformas de reserva suelen gestionarse a través de soluciones de terceros. Cuando se producen incidentes, su resolución rara vez depende de un solo departamento.

El riesgo digital en el turismo suele traspasar los límites de la organización. Las vulnerabilidades en los sistemas de los proveedores, las integraciones mal configuradas o los retrasos en la comunicación pueden aumentar el impacto en todo el ecosistema.

Cooperación interna

Cuando se detecta un problema digital, es fundamental que exista una cooperación estructurada entre el personal operativo y los equipos de TI.

El personal operativo suele ser el primero en observar irregularidades. Sin embargo, la contención técnica requiere conocimientos especializados en TI. Una cooperación eficaz depende de una comunicación clara y de informes precisos.

Al informar de un incidente, el personal debe proporcionar:

- la fecha y la hora de la detección;
- el sistema afectado;
- la cuenta de usuario afectada;
- descripción del comportamiento inusual;
- las medidas ya adoptadas.

Los informes incompletos o imprecisos retrasan la contención y complican la investigación.

Una definición clara de las funciones evita la confusión. El personal operativo informa y conserva la información; el departamento de TI investiga y aísla los sistemas; la dirección coordina las decisiones; y los equipos de cumplimiento normativo o jurídico evalúan las obligaciones reglamentarias.

Una intervención descoordinada por parte de personal no técnico puede ampliar involuntariamente la exposición o comprometer las pruebas.

Cooperación con proveedores externos

Muchas organizaciones turísticas dependen de proveedores de PMS basados en la nube, agencias de viajes en línea (OTA), pasarelas de pago, proveedores de CRM y servicios de TI externalizados. Si un incidente afecta a sistemas alojados externamente, es esencial la comunicación oportuna con los proveedores. Es posible que los proveedores tengan que:

- aislar los servidores afectados;

- desactivar las cuentas comprometidas;
- facilitar los registros del sistema;
- confirmar el alcance de la violación;
- colaborar en la elaboración de informes reglamentarios.

Una notificación tardía a los proveedores puede prolongar la exposición y aumentar el tiempo de inactividad operativa.

Los acuerdos contractuales deben definir claramente:

- las responsabilidades en materia de seguridad;
- los plazos de notificación de incidentes;
- los derechos de acceso;
- las obligaciones en materia de protección de datos;
- los derechos de auditoría y los mecanismos de verificación.

La gobernanza de los proveedores es, por lo tanto, una medida preventiva, no una mera formalidad contractual.

Riesgos de la cadena de suministro y contexto normativo

En el marco de la Directiva NIS2 y las directrices europeas relacionadas con la ciberseguridad, las organizaciones deben gestionar los riesgos no solo dentro de sus propios sistemas, sino también a lo largo de sus cadenas de suministro.

Las empresas turísticas que dependen de proveedores digitales interconectados deben evaluar:

- qué proveedores tratan datos personales;
- qué proveedores tienen acceso directo al sistema;
- qué controles de seguridad se exigen contractualmente;
- cómo se comunican y escalan los incidentes.

Un fallo en un proveedor externo puede convertirse rápidamente en un incidente que afecte a varias organizaciones. La supervisión proactiva de los proveedores reduce el riesgo sistémico.

Documentación y mejora continua

La colaboración debe documentarse en cada fase. Los registros de las comunicaciones con el departamento de TI y los proveedores externos sirven de apoyo para:

Unidad formativa 2: Seguridad digital en el Turismo

- el cumplimiento normativo;
- la revisión de incidentes;
- la identificación de deficiencias en los procedimientos;
- la reducción de riesgos futuros.

La evaluación posterior al incidente debe incluir un análisis de la eficacia de la comunicación y la rapidez de la respuesta. La resiliencia digital depende de la coordinación, no de la actuación individual.

Reflexión y debate

01

¿Por qué es esencial informar con precisión al departamento de TI durante un incidente digital?

02

¿Qué información debe facilitar el personal operativo al escalar un problema?

03

¿Por qué la gobernanza de los proveedores reduce el riesgo sistémico?

7. Tecnologías avanzadas en materia de seguridad del turismo digital

Los entornos de turismo digital dependen cada vez más de tecnologías avanzadas para **reforzar la protección de datos, la verificación de la identidad y la integridad de las transacciones**. Aunque la disciplina operativa sigue siendo esencial, ciertas soluciones tecnológicas pueden reducir significativamente el riesgo sistémico cuando se implementan correctamente.

Las tecnologías de seguridad avanzadas no sustituyen a un comportamiento responsable. Por el contrario, refuerzan los controles existentes y reducen la probabilidad de que las deficiencias humanas o técnicas deriven en incidentes graves.

Blockchain e integridad de los datos

La cadena de bloques es una tecnología de libro mayor distribuido diseñada para mejorar la integridad y la trazabilidad de los datos en entornos digitales con múltiples participantes. Al vincular las transacciones de forma secuencial en una estructura a prueba de manipulaciones, aumenta la transparencia y la rendición de cuentas en los sistemas interconectados.

En los ecosistemas turísticos en los que intervienen múltiples actores —como hoteles, agencias de viajes en línea (OTA) y proveedores de pagos—, la cadena de bloques puede facilitar:

- la verificación de la integridad de los registros de reservas,
- el registro de transacciones a prueba de manipulaciones,
- una mayor confianza en las interacciones con los proveedores.

Los análisis del sector, como el de Mize (2023)¹², sugieren además que la cadena de bloques puede reducir las ineficiencias en la conciliación y mejorar la transparencia transaccional dentro de las redes de distribución de viajes.

Su principal aportación en materia de seguridad radica en la protección de la integridad en entornos digitales compartidos. Sin embargo, la cadena de bloques no aborda vulnerabilidades de comportamiento como el phishing, el uso indebido de credenciales o un control de acceso deficiente. Por lo tanto, su eficacia depende de una mayor madurez en materia de gobernanza, una gestión estructurada de los accesos y una implementación proporcionada basada en la necesidad operativa, más que en la adopción de tendencias tecnológicas.

Identidad digital segura y autenticación sólida

La gestión de la identidad sigue siendo uno de los puntos de control más críticos en el turismo digital. Las credenciales robadas o utilizadas indebidamente suelen servir como puntos de entrada para el fraude y las filtraciones de datos.

Los sistemas de identidad segura pueden incluir:

- autenticación multifactorial (MFA);
- soluciones de identidad federada;
- inicio de sesión único con controles de acceso condicional;
- verificación biométrica en transacciones de alto riesgo.

Una verificación sólida de la identidad reduce el riesgo de apropiación de cuentas y limita el movimiento lateral dentro de los sistemas interconectados. Esto respalda el principio de «Zero Trust» (confianza cero) presentado anteriormente: ninguna confianza implícita, verificación continua.

¹²Ref. Mize. (2023). *Aprovechar el potencial de la tecnología blockchain en el sector de los viajes*.
<https://mize.tech/blog/unlocking-the-potential-of-blockchain-technology-in-travel/>

En los ecosistemas en los que interactúan hoteles, agencias de viajes online (OTA) y proveedores de pagos, la garantía de identidad reduce significativamente el riesgo entre plataformas.

Interconexión de sistemas y seguridad de los ecosistemas

Las tecnologías avanzadas son especialmente relevantes en entornos en los que interactúan múltiples actores digitales. Las plataformas turísticas suelen incluir:

- sistemas de gestión hotelera (PMS);
- agencias de viajes en línea (OTA);
- procesadores de pagos;
- plataformas de marketing;
- proveedores de alojamiento en la nube.

Las medidas de seguridad tecnológicas, como los controles de seguridad de las API, los estándares de cifrado y los sistemas de supervisión automatizados, refuerzan la confianza entre los sistemas interconectados. Sin embargo, la complejidad tecnológica puede generar nuevas dependencias. Una configuración deficiente o una supervisión insuficiente pueden contrarrestar los beneficios previstos.

Evaluación basada en la relación coste-beneficio y en el riesgo

La adopción de tecnologías de seguridad avanzadas debe ser el resultado de una evaluación cuidadosa, más que una reacción a incidentes aislados o a las tendencias del mercado. La implantación de estas tecnologías implica algo más que la adquisición de nuevo software o herramientas. Requiere recursos financieros, integración con los sistemas existentes, formación del personal y ajustes en los procedimientos operativos diarios. En muchos casos, las organizaciones también deben revisar las responsabilidades internas y los mecanismos de gobernanza para garantizar que los nuevos controles funcionen de manera eficaz dentro de los flujos de trabajo existentes.

Una evaluación de costes y beneficios debe examinar tanto los efectos inmediatos como los a largo plazo. Esto incluye la posible reducción de las pérdidas por fraude y de las interrupciones del servicio, las mejoras en el cumplimiento normativo y el refuerzo de la confianza de los clientes. El objetivo no es la complejidad tecnológica, sino una mejora proporcional y demostrable de la resiliencia en materia de seguridad.

No todas las soluciones son igualmente adecuadas para todas las organizaciones. Los operadores más pequeños pueden lograr una protección sustancial reforzando los controles de identidad y los procesos de pago seguros, mientras que las organizaciones más grandes e interconectadas pueden justificar el uso de tecnologías más avanzadas cuando la integridad y la interoperabilidad de todo el sistema son cuestiones estratégicas.

El establecimiento de prioridades basado en el riesgo ayuda a garantizar que las inversiones en seguridad sigan estando en consonancia con la exposición de la organización, la dependencia operativa y el perfil de riesgo general.

El factor humano sigue siendo fundamental

Ni siquiera las tecnologías más avanzadas pueden compensar las prácticas deficientes en materia de contraseñas, la falta de notificación de anomalías, el uso indebido de credenciales o los atajos procedimentales que se toman bajo presión operativa. Estos comportamientos humanos suelen servir de puntos de entrada para los incidentes, independientemente de lo sofisticadas que sean las medidas de protección técnicas.

La tecnología refuerza la resiliencia de la organización solo cuando se apoya en una conducta operativa disciplinada. Los sistemas seguros requieren usuarios responsables. Los controles de identidad, las herramientas de supervisión y los mecanismos de cifrado reducen la exposición, pero no eliminan la necesidad de vigilancia y de cumplimiento de los procedimientos.

La seguridad digital en el turismo es, por lo tanto, tanto técnica como organizativa. La resiliencia sostenible depende de la interacción entre controles tecnológicos estructurados y un comportamiento coherente y responsable en todas las funciones operativas.

Este principio también se aplica al **uso cada vez mayor de herramientas de inteligencia artificial (IA) en el turismo**. Si bien la IA puede facilitar la creación de contenidos, la comunicación con los clientes, el marketing y las tareas operativas, debe **utilizarse de forma responsable** (por ejemplo, evitando la carga de información personal o sensible de los clientes en sistemas públicos de IA) **y de conformidad con las políticas de la organización, los requisitos de protección de datos y la normativa aplicable**. El personal debe verificar los resultados generados por la IA, utilizar servicios de IA aprobados cuando estén disponibles y garantizar que el criterio humano siga siendo fundamental en los procesos de toma de decisiones.

Más allá

Los alumnos analizan cómo las tecnologías de seguridad avanzadas se alinean con marcos estratégicos más amplios, incluidos los principios de «Zero Trust», las expectativas de resiliencia de la cadena de suministro en el marco de la NIS2, el fomento de la confianza digital a largo plazo y la necesidad de escalabilidad en los ecosistemas turísticos interconectados.

Evalúan qué enfoque tecnológico reforzaría de manera más eficaz la resiliencia a nivel del ecosistema, en lugar de centrarse únicamente en la protección de los sistemas individuales.

Reflexión y debate

01

¿Cuál es la principal ventaja de la tecnología blockchain en materia de seguridad?

02

¿Por qué la gestión de la identidad es fundamental para reducir el riesgo digital?

03

¿Por qué la inversión en tecnología debe basarse en el riesgo y no en las tendencias?

04

Más allá: ¿Qué medida de control avanzada mejoraría más la resiliencia sistémica en un ecosistema turístico con múltiples socios?

8. Reflexión y consolidación

Reflexión individual

Los alumnos preparan individualmente respuestas breves por escrito que aborden las siguientes preguntas:

1. ¿Qué etapa del proceso de turismo digital en tu organización conlleva el mayor riesgo digital y por qué?
2. ¿Qué tipo de comportamiento humano representa la mayor vulnerabilidad?
3. ¿Qué mejora concreta reduciría de forma más eficaz el riesgo en tu lugar de trabajo?

Las respuestas deben demostrar que se comprenden las dimensiones operativas, conductuales y normativas del riesgo digital.

Análisis en grupos reducidos

En grupos de tres o cuatro personas, los alumnos comparan sus reflexiones e identifican:

- un proceso compartido de alto riesgo;
- una vulnerabilidad conductual común;
- una mejora que se pudiera implementar de forma realista.

Cada grupo elabora un breve resumen en el que explica su razonamiento. Su análisis debe estructurarse según los siguientes criterios:

- impacto operativo, financiero y reputacional;
- probabilidad de que se produzca;
- posibles implicaciones normativas.

Los grupos presentan brevemente sus conclusiones y justifican las decisiones de priorización.

Escenario: Una escalada durante un fin de semana ajetreado

Es el comienzo de la temporada alta turística. El hotel está completo debido a una gran conferencia internacional que se celebra en la ciudad.

El departamento de contabilidad recibe un correo electrónico urgente de un proveedor habitual en el que se solicita un cambio inmediato de los datos bancarios. El mensaje menciona un «problema de auditoría» y advierte de que, si no se actualiza la información de pago, podrían retrasarse las entregas para el evento.

Debido a la presión operativa y a la disponibilidad limitada de personal, el cambio se procesa sin una verificación adicional.

Dos días después, el departamento de TI detecta una actividad inusual de inicio de sesión en el sistema CRM. Parece que se ha accedido a varios registros de huéspedes fuera del horario laboral habitual, y no está claro si se han exportado datos.

En este momento, el proveedor se pone en contacto con la organización para preguntar por qué no se ha recibido el pago. Al mismo tiempo, el personal de recepción informa de quejas de los huéspedes sobre correos electrónicos sospechosos relacionados con reembolsos. Ante la aparición simultánea de múltiples

irregularidades, la dirección solicita una aclaración urgente y una evaluación inmediata del posible impacto.

La organización se enfrenta ahora a un posible fraude en los pagos y a una filtración de datos, ambos potencialmente relacionados, en plena temporada alta.

Tarea en grupo

En pequeños grupos, los alumnos analizan la situación y esbozan:

1. ¿Cuál debería ser la primera medida inmediata?
2. ¿Qué puestos internos deben intervenir ahora?
3. ¿Qué sistemas deben revisarse o aislarse?
4. ¿Qué información debe documentarse en las primeras 24 horas?
5. ¿Podría esta situación dar lugar a obligaciones de notificación en virtud del RGPD?
6. ¿Qué medida de control previa (proceso, comportamiento o tecnología) podría haber evitado que la situación se agravara?

Los grupos deben justificar sus decisiones teniendo en cuenta el impacto operativo, la exposición financiera, el riesgo normativo y las consecuencias para la reputación.

Puntos de reflexión

Los alumnos deben evaluar cómo la presión operativa influyó en la toma de decisiones y cómo pequeñas desviaciones procedimentales se acumularon hasta convertirse en un incidente de mayor envergadura. Debe prestarse especial atención a la importancia de la verificación temprana, la escalación estructurada y la cooperación coordinada con los equipos de TI y los proveedores.

El debate debe hacer hincapié en cómo los procesos disciplinados protegen tanto al personal como a la organización, especialmente durante los periodos operativos de gran presión.

2.3 Simulaciones y gestión de crisis digitales

Al finalizar esta subunidad, los alumnos serán capaces de reaccionar correctamente ante emergencias digitales, comunicarse de forma clara y responsable, evitar que los daños se agraven y apoyar las medidas de recuperación.

- Tipos de incidentes digitales: phishing y fraude en las reservas, ransomware, DDoS, fugas de datos, apropiación de cuentas
- Jerarquía de comunicación: personal interno, clientes, autoridades (autoridad de protección de datos), medios de comunicación
- Recuperación tras el incidente: restauración del sistema y restablecimiento de la confianza
- Presión psicológica durante una crisis digital

Actividad práctica sugerida:

- Caso práctico 1: ataque de ransomware contra el PMS de un hotel.
- Caso práctico 2: campaña de phishing contra una plataforma de reservas.
- Taller: plan de comunicación para crisis por fuga de datos.

1. Tipos de incidentes digitales en el turismo

Los incidentes digitales se producen cuando los sistemas que gestionan **reservas, pagos o datos de clientes** sufren interrupciones, se utilizan indebidamente o se ven comprometidos. La mayoría de los incidentes siguen una lógica clara de causa y efecto: una vulnerabilidad o un error humano permite el acceso, la interrupción o la manipulación, lo que a su vez genera consecuencias operativas, financieras, legales o para la reputación.

Reconocer las categorías de incidentes permite al personal responder de forma proporcionada en lugar de reaccionar de manera emocional.

Entre los tipos de incidentes más comunes se incluyen:

- **Fugas de datos:** exposición no autorizada de datos personales o de pago, que a menudo conlleva obligaciones normativas y daños a la reputación.
- **Interrupciones del sistema:** indisponibilidad de plataformas críticas debido a fallos técnicos o ataques, lo que provoca la interrupción del servicio y la pérdida de ingresos.

- **Incidentes de pago:** transacciones fraudulentas, cobros incorrectos o devoluciones que afectan a la estabilidad financiera.
- **Acceso no autorizado:** acceso a sistemas o datos sin la autorización correspondiente, lo que aumenta el riesgo de manipulación o filtración.
- **Manipulación de la reputación o desinformación:** información errónea coordinada que afecta a la confianza y al comportamiento a la hora de realizar reservas.

Cada tipo de incidente afecta de manera diferente a las partes interesadas. Los clientes pueden sufrir perjuicios económicos o en materia de privacidad; el personal puede enfrentarse a presiones operativas y a obligaciones de notificación; y la dirección debe hacer frente a los riesgos normativos y de reputación.

Una respuesta eficaz comienza con una notificación rigurosa, una escalación estructurada y una comunicación controlada.

Más allá

Clasificar los incidentes según **su gravedad y el alcance de su impacto** permite establecer prioridades de forma proporcionada. Los incidentes de baja gravedad pueden gestionarse a nivel local, mientras que los de alta gravedad que impliquen datos sensibles, perturbaciones sistémicas o exposición a riesgos normativos requieren una escalación inmediata, supervisión por parte de la alta dirección y una gestión coordinada de la crisis.

Sin embargo, la gravedad no debe evaluarse de forma estática. Los incidentes digitales en entornos turísticos suelen evolucionar progresivamente a través de etapas de escalada identificables:

1. **Detección de anomalías:** se observa una irregularidad menor o un comportamiento inusual del sistema
2. **Compromiso local:** afecta de forma limitada a un sistema, una cuenta o un dispositivo
3. **Movimiento lateral:** propagación a través de sistemas interconectados o cuentas de usuario
4. **Perturbación operativa:** interrupción del servicio, pérdidas económicas o fallos en las reservas
5. **Escalada normativa y reputacional:** intervención de las autoridades de supervisión, notificación a los clientes, exposición pública

Unidad formativa 2: Seguridad digital en el Turismo

Reconocer estas fases de agravamiento permite intervenir antes, limita la propagación sistémica y respalda una toma de decisiones regulatoria defendible. La identificación proactiva en la fase de anomalía o de compromiso local reduce significativamente el daño operativo y reputacional.

Reflexión y debate

01

Nombra dos tipos de incidentes digitales y una posible consecuencia de cada uno.

02

¿Por qué es esencial la elaboración de informes estructurados durante un incidente?

03

Más allá: ¿Cómo mejora la clasificación de la gravedad la toma de decisiones?

2. La presión psicológica en las crisis digitales

Las crisis digitales rara vez se desarrollan en condiciones tranquilas. El estrés, la incertidumbre y la presión del tiempo reducen la atención y aumentan la probabilidad de que se tomen atajos en los procedimientos. La sobrecarga cognitiva puede hacer que el personal se salte pasos de verificación o actúe de forma precipitada, lo que podría ampliar el impacto del incidente.

Las investigaciones sobre factores humanos y ciberseguridad demuestran de forma sistemática que el estrés, la sobrecarga cognitiva y la presión del tiempo aumentan significativamente la probabilidad de que se produzcan errores de procedimiento durante la respuesta a incidentes, lo que refuerza la necesidad de una escalación estructurada y de roles predefinidos¹³.

La falta de una escalación temprana —tal y como se analiza en las subunidades 2.1 y 2.2— suele ser un desencadenante sistémico de la agravación de la crisis. Bajo presión psicológica, los intentos correctivos individuales a menudo socavan la respuesta estructurada y aumentan el impacto a largo plazo.

¹³ Agencia de la Unión Europea para la Ciberseguridad (ENISA). (2019). *Directrices sobre la cultura de la ciberseguridad: aspectos conductuales de la ciberseguridad*. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>

Unidad formativa 2: Seguridad digital en el Turismo

Los procedimientos estructurados mitigan estos riesgos. Unas vías de escalado claras, unas responsabilidades bien definidas y unas breves listas de verificación para la toma de decisiones reducen la ambigüedad. Un gestor de incidentes designado centraliza la coordinación y limita las acciones contradictorias.

Entre las medidas prácticas de estabilización se incluyen:

- protocolos de «pausa y verificación» antes de llevar a cabo acciones irreversibles;
- rutinas de notificación ensayadas;
- el apoyo visible de los responsables, que fomente la escalación temprana;
- reuniones de análisis posteriores al incidente para reforzar el aprendizaje.

La resiliencia ante las crisis depende tanto de la disciplina conductual como de la capacidad técnica.

Ir más allá

Los líderes deben establecer umbrales de decisión que definan cuándo es obligatorio escalar el asunto de forma inmediata. Las herramientas de apoyo a la toma de decisiones, como los modelos RACI simplificados o las matrices de escalación, facilitan una actuación coherente en situaciones de estrés. Un liderazgo eficaz equilibra la rapidez con la conservación de las pruebas y el bienestar del personal.

Reflexión y debate

01

Identifica dos factores psicológicos que aumentan el riesgo de cometer errores durante una crisis.

02

¿Por qué es preferible la escalación a la resolución individual de problemas en situaciones de gran presión?

03

Más allá: ¿Cómo puede el liderazgo estructurar la toma de decisiones para mantener tanto la rapidez como la precisión?

3. Caso práctico 1: Ataque de ransomware contra el sistema de gestión hotelera (PMS) de un hotel

Actividad práctica

Unidad formativa 2: Seguridad digital en el Turismo

Objetivo: Demostrar una respuesta coordinada ante incidentes bajo presión operativa.

Formato: Simulación en grupo basada en roles

Duración estimada: 60-90 minutos

Esta actividad permite a los alumnos aplicar los principios de gestión de crisis en un escenario simulado de ataque de ransomware. Los participantes practican la escalación estructurada, la toma de decisiones coordinada, la evaluación normativa y la comunicación bajo presión operativa.

Un hotel de una ciudad de tamaño medio sufre un ataque de ransomware durante la noche. Cuando llega el turno de mañana, el personal no puede acceder al sistema de gestión hotelera (PMS). Los registros de reservas están cifrados, los pagos automáticos han fallado y no se pueden verificar las preautorizaciones de tarjetas. En cuestión de minutos comienzan a formarse colas para el registro de entrada.

La investigación inicial revela que el ataque se originó a partir de un correo electrónico de phishing abierto durante el turno de noche. El malware se ejecutó en una estación de trabajo conectada a la red del PMS. Debido a que la segmentación de la red era insuficiente, el código malicioso se propagó lateralmente a los sistemas de copia de seguridad compartidos, dejándolos temporalmente inutilizables.

El impacto operativo es inmediato y va en aumento. El personal de recepción recurre a procedimientos de registro manuales. Los huéspedes expresan su frustración por los retrasos. Los equipos financieros no pueden confirmar las transacciones. La dirección debe decidir si bloquear por completo el acceso externo, lo que podría agravar la interrupción operativa.

En cuestión de horas, el hotel se enfrenta a múltiples capas de exposición interrelacionadas. Las operaciones centrales de reservas quedan paralizadas, lo que interrumpe los registros de entrada y las reservas. Las pérdidas económicas comienzan a acumularse debido a las reservas canceladas y a las devoluciones de cargos. Al mismo tiempo, si se ha visto comprometida la integridad de los datos personales, pueden surgir obligaciones reglamentarias de notificación. El daño a la reputación se agrava rápidamente a medida que los huéspedes comparten sus quejas y preocupaciones en Internet, lo que amplifica el impacto más allá del fallo operativo inmediato.

La contención requiere el aislamiento rápido de los sistemas infectados, la restricción del acceso a la red, la intervención de especialistas forenses externos y la verificación de copias de seguridad limpias antes de la restauración. La recuperación se prolonga

durante varias semanas y exige esfuerzos coordinados a nivel técnico, operativo y de comunicación.

Evaluación inicial de la situación

Los alumnos trabajan en pequeños grupos. Deben:

- identificar los riesgos inmediatos operativos, financieros, normativos y de reputación;
- determinar si el incidente puede considerarse una posible violación de datos personales;
- definir la primera medida operativa que debe adoptarse en los primeros 30 minutos.

Los grupos presentan breves justificaciones basadas en el impacto y la lógica de escalado.

Coordinación de crisis basada en funciones

A los alumnos se les asignan funciones organizativas específicas:

- Responsable de operaciones
- Responsable de TI
- Responsable de finanzas
- Responsable de comunicaciones
- Responsable de cumplimiento normativo y protección de datos

Cada grupo debe ponerse de acuerdo sobre:

- las medidas de contención inmediatas;
- las decisiones sobre el aislamiento del sistema;
- si se requiere apoyo forense externo;
- si debe iniciarse la evaluación de riesgos normativos;
- las prioridades de comunicación interna.

Cada función describe brevemente sus principales preocupaciones y prioridades a la hora de tomar decisiones. El objetivo es demostrar una actuación coordinada en lugar de respuestas aisladas.

Escalada ante la presión pública

El formador presenta nuevos acontecimientos:

- Los medios de comunicación sugieren que se ha producido un «fallo del sistema en el hotel».
- Un huésped cuestiona públicamente si se han visto comprometidos los datos de pago.

Los grupos deben decidir:

- qué información se puede comunicar de inmediato;
- qué debe seguir siendo objeto de investigación;
- quién actúa como portavoz;
- si deben iniciarse los procedimientos de notificación externa.

Las decisiones deben encontrar un equilibrio entre la transparencia y las consideraciones legales y forenses.

Causa raíz y estrategia preventiva

Los grupos llevan a cabo un análisis breve y estructurado:

- ¿Qué fallo permitió que el incidente se agravara?
- ¿Qué control técnico reduciría en mayor medida la posibilidad de que se repita?
- ¿Qué mejora en el comportamiento o en los procedimientos es necesaria?
- ¿Qué proveedor o elemento de gobernanza contribuyó a la exposición al riesgo?

Los grupos establecen un orden de prioridad de las medidas correctivas basándose en la reducción del riesgo sistémico.

Más allá

Un análisis estructurado de las causas raíz identifica tres debilidades sistémicas: el éxito de los ataques de phishing, una segmentación inadecuada de la red y la ubicación de las copias de seguridad en el mismo entorno accesible. Las prioridades correctivas incluyen:

- el refuerzo del filtrado de correo electrónico y las pruebas de concienciación sobre el phishing;
- mejora de la segmentación de la red para evitar la propagación lateral;
- la implementación de copias de seguridad fuera de línea o inmutables;
- reforzo de los protocolos de escalado para garantizar una detección y notificación más tempranas.

La aplicación de un método de revisión estructurado (cronología de incidentes → identificación de las causas raíz → plan de corrección priorizado) garantiza que las lecciones aprendidas se traduzcan en mejoras cuantificables de la resiliencia, en lugar de en soluciones temporales.

4. Caso práctico 2: campaña de phishing en una plataforma de reservas

Actividad práctica

Objetivo: Analizar cómo debe responder una empresa turística cuando sus huéspedes se convierten en blanco de una campaña de phishing.

Formato: Debate en grupo y ejercicio de resolución de problemas

Duración estimada: 45-60 minutos

Esta actividad permite a los alumnos analizar un incidente de phishing que afecta a los huéspedes a través de una plataforma de reservas de confianza. Los participantes practican la evaluación de riesgos, la comunicación con los clientes, la coordinación con socios externos y la planificación de la respuesta.

Un pequeño hotel empieza a recibir llamadas de huéspedes que han recibido mensajes en los que se les pide que realicen un pago adicional para confirmar su reserva. Los mensajes parecen proceder de una conocida plataforma de reservas e incluyen un enlace a una página de pago.

Varios huéspedes siguen las instrucciones e introducen sus datos de pago antes de darse cuenta de que los mensajes son fraudulentos.

El hotel se pone en contacto con la plataforma de reservas y descubre que los atacantes podrían haber obtenido acceso a una de las cuentas de la plataforma utilizadas para comunicarse con los huéspedes. A medida que llegan más denuncias, los huéspedes comienzan a publicar advertencias en las redes sociales y en sitios web de opiniones. El personal del hotel no sabe muy bien cuánta información debe facilitar ni cómo debe responder a los clientes preocupados.

Evaluación inicial

En pequeños grupos, debatid:

- ¿Cuáles son los principales riesgos para los huéspedes?
- ¿Cuáles son los principales riesgos para el hotel?

- ¿De qué información se dispone ya?
- ¿Qué información adicional se necesita antes de poder tomar decisiones?
- ¿Qué se debe hacer durante las primeras horas tras detectarse el incidente?

Gestión de la situación

Vuestro grupo representa al equipo directivo del hotel.

Debatid y poneros de acuerdo sobre:

- ¿Cómo se debe informar a los huéspedes sobre el incidente?
- ¿Qué consejos se deben dar a los huéspedes afectados?
- ¿Quién debe comunicarse con la plataforma de reservas?
- ¿Debería emitirse un comunicado público?
- ¿Qué medidas pueden ayudar a mantener la confianza de los clientes?

Elabora un breve plan de acción y explica tus decisiones.

Revisión y prevención

Tras debatir el escenario, reflexiona sobre las siguientes preguntas:

- ¿Por qué era probable que los huéspedes confiaran en los mensajes?
- ¿Qué señales de alerta podrían haber indicado que los mensajes eran fraudulentos?
- ¿Qué medidas podrían ayudar a prevenir incidentes similares en el futuro?
- ¿Cómo pueden las empresas turísticas ayudar a los huéspedes a reconocer los intentos de phishing?

Más allá

Este caso demuestra que los incidentes cibernéticos no siempre se originan en los propios sistemas de una organización. Las empresas turísticas suelen depender de plataformas de reserva, proveedores de pagos y otros socios digitales. Cuando una parte de este ecosistema se ve afectada, los clientes pueden seguir asociando el problema con el proveedor de alojamiento.

Entre las medidas que pueden reducir el riesgo se incluyen:

- activar la autenticación multifactorial para las cuentas de la plataforma;
- revisar periódicamente la actividad de las cuentas;
- impartir formación al personal sobre los riesgos del phishing;
- informar a los huéspedes sobre los procedimientos oficiales de pago;

- establecer procedimientos de comunicación claros para incidentes digitales.

Este escenario pone de relieve la importancia de la comunicación con los clientes, la seguridad de las plataformas de terceros y el mantenimiento de la confianza durante un incidente digital.

5. Comunicación en situaciones de crisis

Por qué la comunicación determina el resultado de una crisis

Durante un incidente digital, la comunicación no es secundaria respecto a la respuesta técnica; es un elemento central de la gestión de crisis. La forma en que se comparte la información influye en la rapidez de la contención, el cumplimiento normativo, la confianza de las partes interesadas y la confianza a largo plazo en la organización. Unos mensajes mal estructurados o informales pueden convertir rápidamente un incidente técnico en una crisis de reputación más amplia.

Cuando la comunicación carece de coordinación, aumenta la confusión interna. El personal puede recibir instrucciones contradictorias, pueden producirse acciones duplicadas y pueden llegar declaraciones prematuras a los huéspedes o a los medios de comunicación. Esto no solo ralentiza la contención, sino que también puede aumentar el riesgo legal y dañar la confianza del público. Por este motivo, la comunicación de crisis debe ser disciplinada, proporcionada y coordinada estratégicamente.

Principios básicos de la comunicación

Una comunicación de crisis eficaz en el sector turístico se basa en cinco principios:

1. **Precisión antes que rapidez:** verificar los hechos antes de su divulgación pública.
2. **Un único punto de autoridad:** designar a un portavoz.
3. **La coordinación interna es lo primero:** asegúrate de que el personal comprenda la situación antes de enviar mensajes al exterior.
4. **Transparencia sin especulaciones:** comunicar lo que se sabe y evitar las suposiciones.
5. **Registro documentado de la comunicación:** conservar los registros para su revisión legal y normativa.

Estructura de comunicación interna

Inmediatamente después de que se detecte un incidente, **los equipos pertinentes** deben recibir un informe conciso y basado en hechos. Este informe debe aclarar **qué se ha confirmado, qué sigue bajo investigación, qué medidas inmediatas son necesarias y quién está autorizado a comunicarse con el exterior**.

Una comunicación interna clara reduce la incertidumbre y evita acciones no autorizadas. En situaciones de gran presión, el personal puede sentirse obligado a «solucionar» los problemas por su cuenta o a responder de manera informal a las consultas de los huéspedes. Una coordinación interna estructurada mitiga estos riesgos y protege tanto al personal como la credibilidad de la organización.

Comunicación externa con los huéspedes

La comunicación con los huéspedes debe equilibrar la claridad, la empatía y la precisión de los hechos. Los mensajes deben explicar el **impacto operativo del incidente**, describir **las medidas inmediatas que se están tomando** y proporcionar **orientación práctica o canales de apoyo**. El tono debe ser tranquilo y responsable, evitando un lenguaje a la defensiva o conclusiones prematuras.

Las declaraciones especulativas pueden generar riesgos legales y reputacionales adicionales, especialmente en los casos en los que aún no se haya confirmado la integridad de los datos personales. Por lo tanto, es esencial mantener la coherencia en todos los canales de comunicación. Las actualizaciones contradictorias procedentes de distintos departamentos pueden socavar significativamente la confianza.

Accesibilidad digital en la comunicación de crisis

Las estrategias de comunicación de crisis deben **garantizar que la información llegue a todos los huéspedes, incluidos aquellos con discapacidades visuales, auditivas o cognitivas**. Durante los incidentes digitales, depender de un único canal de comunicación puede excluir a determinados grupos, especialmente si los sistemas se ven afectados.

Una comunicación accesible requiere el uso de múltiples formatos complementarios, tales como:

- señalización visual clara en recepción o en las zonas comunes;
- explicaciones verbales o comunicación asistida por el personal;
- anuncios de audio cuando sea pertinente;

- mensajes escritos en un lenguaje sencillo y claro.

Por ejemplo, si no se dispone de pantallas digitales o notificaciones en el móvil, la señalización física o la comunicación directa con el personal pueden convertirse en el método principal para informar a los huéspedes. Garantizar la accesibilidad en situaciones de crisis no es solo una cuestión de calidad del servicio, sino también de seguridad, inclusión y responsabilidad legal.

Comunicación y cumplimiento normativo

En incidentes que puedan implicar datos personales, la comunicación se entrecruza directamente con las obligaciones normativas. En el marco del RGPD (artículos 33 y 34 del RGPD), **la notificación a las autoridades de control** y, cuando sea necesario, **a las personas afectadas**, debe basarse en una evaluación estructurada y no en una reacción emocional. Por lo tanto, los mensajes públicos deben ajustarse al asesoramiento jurídico para garantizar el cumplimiento normativo, al tiempo que se preserva la integridad de la investigación.

Una comunicación transparente demuestra responsabilidad; sin embargo, una divulgación prematura puede comprometer las pruebas forenses o agravar la responsabilidad. El equilibrio entre transparencia y control es una responsabilidad fundamental del liderazgo durante la gestión de crisis.

Actividad práctica: simulación de comunicación

Objetivo: Redactar comunicaciones estructuradas, tanto internas como externas, durante un incidente digital.

Formato: Tarea de redacción en grupos reducidos

Duración estimada: 45 minutos

Los alumnos trabajan en pequeños grupos para redactar tres mensajes breves basados en un incidente simulado:

1. Un breve informe interno (máx. 150 palabras).
2. Un comunicado provisional dirigido al público.
3. Una respuesta a una consulta de los medios de comunicación.

Cada grupo debe justificar qué información se ha incluido, qué se ha omitido intencionadamente y cómo las consideraciones normativas han influido en la elección de la redacción. Se hace hincapié no solo en el contenido, sino también en el razonamiento y la proporcionalidad.

Más allá: la comunicación de crisis como ciclo estructurado

La gestión avanzada de crisis reconoce que la comunicación evoluciona a través de fases distintas, en lugar de producirse como una única reacción. En los incidentes digitales, la comunicación suele seguir cuatro etapas: **preparación, respuesta inmediata, estabilización y restablecimiento de la confianza**.

La preparación implica funciones predefinidas, plantillas y vías de escalación. La respuesta inmediata se centra en la coordinación interna y en la difusión controlada de mensajes externos. La estabilización requiere actualizaciones constantes y coordinación con las autoridades reguladoras. La reconstrucción de la confianza va más allá de la recuperación técnica y hace hincapié en medidas correctivas visibles y en la tranquilidad a largo plazo.

Entender la comunicación como un ciclo ayuda a las organizaciones a evitar los mensajes reactivos y a mantener el control estratégico durante las crisis digitales.

Reflexión y debate

01

¿Cuál debería ser el primer paso en materia de comunicación interna

02

¿Por qué la comunicación con los huéspedes debe evitar las

6. Recuperación tras el incidente y confianza

Tras un incidente digital, la recuperación debe ser **rápida y estructurada**. Las decisiones iniciales determinan si la interrupción se contiene de manera eficiente o si deriva en una inestabilidad prolongada. La prioridad inicial es la estabilización técnica: **aislar los sistemas afectados, restaurar copias de seguridad verificadas y limpias, y proteger los puntos de acceso para evitar que se repita**.

Sin embargo, la recuperación va más allá de la reparación técnica. La gestión de la recuperación debe seguir los principios de respuesta estructurada descritos en las secciones anteriores. Las medidas correctivas fragmentadas o no documentadas debilitan la resiliencia a largo plazo y pueden exponer a la organización a una revisión regulatoria secundaria. Por lo tanto, **una recuperación eficaz** combina la restauración técnica con una documentación rigurosa, una evaluación regulatoria y una comunicación transparente.

Las medidas fundamentales de recuperación incluyen:

- verificar la integridad de las copias de seguridad antes de la restauración;
- aplicar controles compensatorios a corto plazo para reducir el riesgo residual;
- realizar un análisis forense específico para confirmar el alcance y el impacto;
- documentar todas las acciones a efectos de cumplimiento normativo y auditoría.

Una vez estabilizados los sistemas, la atención se centra en restablecer la confianza. Para ello se requieren medidas coherentes y creíbles, más allá de las simples palabras de tranquilidad. Las organizaciones deben **comunicar con claridad las medidas correctivas**, demostrar las mejoras en materia de seguridad —como el refuerzo de los controles de acceso o la segmentación— y **proporcionar canales de contacto accesibles para las partes interesadas afectadas**.

El apoyo al personal también es fundamental durante la recuperación. La fatiga y la presión operativa aumentan la probabilidad de que se produzcan errores secundarios. Los horarios estructurados, la asignación clara de tareas y la formación tras el incidente refuerzan la resiliencia y demuestran la responsabilidad de la organización.

Una recuperación sostenible integra la corrección técnica, el refuerzo de la gobernanza y la reconstrucción de la confianza. Cuando se gestiona adecuadamente, la fase de recuperación se convierte en una oportunidad para fortalecer la resiliencia a largo plazo, en lugar de limitarse a restablecer las condiciones anteriores.

Más allá

La planificación avanzada de la recuperación va más allá de la estabilización inmediata. La reconstrucción de la confianza a largo plazo puede incluir medidas de verificación independientes, como auditorías o certificaciones de terceros, actualizaciones estructuradas sobre la transparencia dirigidas a clientes y socios, mecanismos reforzados de garantía de los proveedores e inversión en supervisión continua y en una arquitectura de copias de seguridad resiliente (incluidas las copias de seguridad inmutables).

Estas medidas garantizan que la recuperación no sea reactiva, sino transformadora. La inversión estratégica tras un incidente debe ser proporcional al tamaño y la

exposición de la organización, equilibrando el coste con reducciones cuantificables del riesgo futuro y la vulnerabilidad reputacional.

Reflexión y debate

01

Identifica tres prioridades inmediatas durante la fase de recuperación. Explica por qué estas acciones deben abordarse antes de que comiencen las mejoras a largo plazo.

02

¿Por qué es esencial la documentación estructurada de las medidas de recuperación? Considera su papel en el cumplimiento normativo, el aprendizaje interno, la rendición de cuentas y la confianza de las partes interesadas.

03

¿Qué medidas a largo plazo son más eficaces para restablecer la confianza digital en una organización turística? Evalúa si las actualizaciones técnicas, las medidas de transparencia, las auditorías independientes, las garantías de los proveedores o la formación del personal tienen el mayor impacto a largo plazo, y justifica tu razonamiento.

Perspectiva final: la seguridad digital como gobernanza

La seguridad digital en el turismo no debe entenderse como una función puramente técnica, sino como una disciplina de gobernanza integrada que combina la vigilancia operativa, el conocimiento de la normativa, la priorización estructurada de riesgos y la gestión coordinada de crisis. La resiliencia sostenible surge de prácticas diarias disciplinadas respaldadas por controles tecnológicos proporcionados.

7. Debate final y evaluación

Ejercicio: Debate de consolidación reflexiva

Objetivo: Consolidar la comprensión conceptual y fomentar la autoevaluación de la responsabilidad profesional en entornos de seguridad digital.

Formato: Reflexión en grupo

Unidad formativa 2: Seguridad digital en el Turismo

Duración estimada: 20-30 minutos

Los participantes debaten los siguientes puntos de reflexión y los relacionan con contextos operativos reales del sector turístico:

- ¿Cómo reconocerías que un problema técnico o relacionado con los datos se está convirtiendo en un incidente digital?
- ¿En qué momento se debe escalar un problema en lugar de gestionarlo de forma individual?
- ¿Cómo ayudan los procedimientos y la documentación en situaciones de gran presión?
- ¿Qué comportamientos comunicativos ayudan a proteger la confianza de los clientes durante y después de los incidentes?
- ¿Cómo influye tu propio comportamiento en tus compañeros, en los clientes y en los resultados de la recuperación?

Cuestionario de evaluación final

Objetivo: Evaluar la comprensión teórica y la competencia en la toma de decisiones aplicada en todos los componentes de la Unidad 2.

Formato: Evaluación individual

Duración estimada: 25-35 minutos

Preguntas:

1. Cuando se sospecha de un incidente digital, ¿qué medida se debe tomar en primer lugar?

- A. Intentar resolver el problema por cuenta propia antes de informar a los demás
- B. Esperar hasta disponer de una confirmación técnica completa
- C. Escalar el incidente inmediatamente a través del canal de notificación establecido
- D. Informar a los huéspedes antes de notificarlo a los equipos internos

Respuesta correcta: C

2. ¿Qué concepto del curso refuerza más directamente la responsabilidad personal en materia de seguridad digital?

- A. Estándares avanzados de cifrado
- B. Los principios de «Zero Trust» y la disciplina de escalación temprana
- C. Mecanismos de verificación de blockchain
- D. Plantillas de comunicación con los medios

Respuesta correcta: B

3. ¿Por qué la comunicación estructurada reduce el impacto de los incidentes digitales?

- A. Elimina la necesidad de contención técnica
- B. Evita la confusión, la duplicación de acciones y el deterioro de la reputación
- C. Sustituye a los requisitos normativos de notificación
- D. Garantiza que los incidentes se mantengan confidenciales

Respuesta correcta: B

4. ¿Qué comportamiento reduce de forma más significativa el riesgo digital en las operaciones cotidianas?

- A. Compartir las credenciales únicamente con compañeros de confianza
- B. Ignorar las anomalías menores durante los periodos de mayor actividad
- C. Notificar las actividades sospechosas lo antes posible y seguir los procedimientos
- D. Confiar exclusivamente en el departamento de TI para detectar amenazas

Respuesta correcta: C

5. ¿En qué momento debe elevarse un problema operativo como posible incidente digital?

- A. Solo después de que los clientes se quejen
- B. Cuando exista una sospecha razonable de que los datos se han visto comprometidos o de que se ha hecho un uso indebido del sistema
- C. Después de solicitar la aprobación de la dirección
- D. Cuando se involucren los medios de comunicación

Respuesta correcta: B

6. ¿Qué práctica refuerza de forma más eficaz la resiliencia digital a largo plazo?

- A. Restaurar los sistemas rápidamente sin documentación
- B. Realizar un análisis de las causas raíz e implementar mejoras estructurales
- C. Minimizar la comunicación para evitar daños a la reputación
- D. Tratar los incidentes como fallos técnicos aislados

Respuesta correcta: B

7. ¿Qué comportamiento comunicativo protege la confianza de los clientes durante una crisis?

- A. Proporcionar explicaciones técnicas detalladas de inmediato
- B. Especular sobre las posibles causas para dar una imagen de transparencia
- C. Ofrecer información actualizada, contrastada, coherente y empática
- D. Evitar las declaraciones públicas hasta que la investigación haya concluido por completo

Respuesta correcta: C

8. ¿Qué combinación refleja mejor un enfoque de recuperación disciplinado?

- A. Reinicio rápido del sistema, documentación mínima, comunicación retrasada
- B. Contención técnica, acciones documentadas, evaluación normativa, mensajes coordinados

- C. Disculpa pública antes de confirmar el impacto
- D. Aislamiento de las TI de la toma de decisiones de la dirección

Respuesta correcta: B

9. ¿Cuáles son los DOS factores que con mayor frecuencia hacen que un problema menor se convierta en una crisis digital?

- A. Retraso en la escalación debido a la incertidumbre
- B. Comunicación inmediata y transparente a los reguladores
- C. Atajos en los procedimientos bajo presión operativa
- D. Una fuerte segmentación de la red

Respuestas correctas: A y C

10. ¿Qué DOS elementos son esenciales para un cumplimiento normativo eficaz durante un incidente relacionado con datos personales?

- A. Comunicado de prensa inmediato
- B. Documentación estructurada de las medidas adoptadas
- C. Evaluación de riesgos del impacto en las personas
- D. Eliminación interna de los registros sospechosos

Respuestas correctas: B y C

11. ¿Cuáles son las DOS medidas que reducen de forma más eficaz la probabilidad de que el ransomware se propague por los sistemas?

- A. Segmentación de la red
- B. Compartir las credenciales de administrador únicamente dentro del equipo directivo
- C. Copias de seguridad fuera de línea o inmutables
- D. Evitar la comunicación con especialistas forenses externos

Respuestas correctas: A y C

12. ¿Qué DOS prácticas de comunicación refuerzan la credibilidad de la organización durante una crisis?

- A. Un único portavoz autorizado
- B. Varios departamentos que responden de forma independiente
- C. Mensajes coherentes en todos los canales
- D. Divulgación inmediata de detalles técnicos no verificados

Respuestas correctas: A y C

13. ¿Qué DOS comportamientos demuestran una gran responsabilidad profesional en entornos de turismo digital?

- A. Notificar las anomalías aunque no se tenga certeza
- B. Intentar resolver las posibles infracciones de forma independiente
- C. Seguir los procedimientos de escalado definidos
- D. Esperar instrucciones directas de la dirección antes de actuar

Respuestas correctas: A y C

1. Comisión Europea. (2024). *El Pacto de la UE por las Competencias: Alianza para las Competencias en el Ecosistema Turístico (Actualización de la situación de partida)*. <https://pact-for-skills.ec.europa.eu/>
2. Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre los servicios de pago en el mercado interior (PSD2). (2015). *Diario Oficial de la Unión Europea*, L 337. <https://eur-lex.europa.eu/eli/dir/2015/2366/oj>
3. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (Reglamento General de Protección de Datos). (2016). *Diario Oficial de la Unión Europea*, L 119. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
4. Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a la ENISA (Agencia de Ciberseguridad de la Unión Europea) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Ley de Ciberseguridad). (2019). *Diario Oficial de la Unión Europea*, L 151. <https://eur-lex.europa.eu/eli/reg/2019/881/oj>
5. Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para un nivel común elevado de ciberseguridad en toda la Unión (Directiva NIS2). (2022). *Diario Oficial de la Unión Europea*, L 333. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
6. Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre la gobernanza europea de los datos (Ley de Gobernanza de los Datos). (2022). *Diario Oficial de la Unión Europea*, L 152. <https://eur-lex.europa.eu/eli/reg/2022/868/oj>
7. Agencia de Ciberseguridad de la Unión Europea (ENISA). (2022). *Directrices sobre la cultura de la ciberseguridad: aspectos conductuales de la ciberseguridad*. <https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity>

8. Agencia de Ciberseguridad de la Unión Europea (ENISA). (2025). *Guía técnica de implementación sobre medidas de gestión de riesgos de ciberseguridad (Versión 1.0)*. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
9. Organización Internacional de Normalización y Comisión Electrotécnica Internacional. (2022). *ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. <https://www.iso.org/standard/27001>
10. Organización Mundial del Turismo (OMT). (s. f.). *Código ético mundial del turismo*. <https://www.untourism.int/global-code-of-ethics-for-tourism>



 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