

Q&A WEBINAR “¿QUÉ HACER SI UN HOTEL SUFRE UN PHISHING? RESPONSABILIDAD, FRAUDE Y BRECHAS DE DATOS”

1 de octubre de 2026

Como complemento al WEBINAR “¿QUÉ HACER SI UN HOTEL SUFRE UN PHISHING? RESPONSABILIDAD, FRAUDE Y BRECHAS DE DATOS” organizado por **Tourism&Law**, en colaboración con **CEHAT** el pasado 28 de septiembre de 2026, procedemos a recoger en el presente documento las cuestiones que fueron trasladadas antes y durante el mismo por los asistentes, con objeto de proceder a su respuesta y facilitar su difusión entre ellos.

A tal efecto, se han extraído y anonimizado los hechos comunicados por los participantes en sus consultas para extraer de estas pautas y orientaciones que complementen lo expuesto durante la sesión con un alcance generalizado.

1. Si se vulnera el motor de reservas o el PMS, ¿quién es responsable?

Que la brecha se produzca en los sistemas del proveedor no significa que este deba asumir todas las obligaciones ni que el hotel pueda desentenderse de lo ocurrido. Cuando el establecimiento decide para qué y cómo deben utilizarse los datos de sus reservas y el proveedor los gestiona por su cuenta y siguiendo sus instrucciones, el hotel actúa como responsable del tratamiento y el proveedor como encargado. Para comprobar que esa es la relación existente, deben examinarse las funciones que desempeña cada parte y el contrato, sin que resulte determinante quién sea el propietario de los servidores o dónde estén alojados.

En esa relación, cada parte tiene obligaciones propias. El proveedor debe aplicar medidas de seguridad adecuadas, informar al hotel de la brecha sin dilación indebida y facilitar la información y asistencia necesarias para gestionarla. Por su parte, el hotel debe evaluar el riesgo para los afectados, documentar lo sucedido y asegurar que se realizan las notificaciones y comunicaciones legalmente exigibles. La gestión debe ser coordinada, pero la intervención del proveedor no sustituye las obligaciones del establecimiento. Tampoco puede el proveedor eludir sus compromisos frente al hotel alegando que el fallo corresponde a otra empresa a la que subcontrató el tratamiento.

Ahora bien, que el hotel conserve esas obligaciones no significa que sea automáticamente culpable del ataque ni que deba indemnizar cualquier perjuicio. La existencia de una brecha no demuestra, por sí sola, que las medidas de seguridad fueran inadecuadas: habrá que examinar cómo se produjo el incidente y qué actuaciones correspondían a cada parte. En ese análisis, el hotel deberá poder acreditar las garantías exigidas al proveedor, las medidas que le correspondía

adoptar y su reacción al conocer la brecha. La intervención de delincuentes no basta, por sí misma, para quedar exonerado.

Si un huésped reclama una indemnización conforme al artículo 82 del RGPD, deberán concurrir una infracción de la normativa, un daño material o inmaterial y una relación causal entre ambos. Por tanto, la obligación de gestionar la brecha y la obligación de indemnizar son cuestiones distintas: la primera debe atenderse desde que se conoce el incidente, mientras que la segunda dependerá de los incumplimientos y daños que se acrediten.

Cuando hotel y proveedor hayan participado en el mismo tratamiento y ambos resulten jurídicamente responsables del daño, el afectado podrá reclamar su reparación íntegra a cualquiera de ellos. Quien abone la indemnización podrá después reclamar al otro la parte correspondiente a su responsabilidad. Con independencia de esa reclamación del huésped, el hotel también podrá exigir al proveedor los daños derivados de un incumplimiento contractual, siempre que concurran los requisitos para ello. En consecuencia, la responsabilidad deberá determinarse a partir de lo que cada parte debía hacer, lo que efectivamente hizo y cómo influyó su actuación en el perjuicio.

2. ¿Qué protocolo debe seguir el hotel cuando el incidente se produce en un proveedor?

El hotel debe activar su respuesta sin esperar a que el proveedor cierre la investigación. Conviene designar un coordinador, incorporar al equipo técnico y al asesor de protección de datos o delegado de protección de datos (DPD), si existe, y pedir un primer informe sobre las cuentas, datos, reservas y periodos afectados. La petición debe incluir la preservación inmediata de evidencias.

La contención técnica debe desarrollarse en paralelo: revisar accesos, revocar sesiones o credenciales comprometidas y valorar la suspensión de las conexiones afectadas. En una integración mediante API (la conexión entre los sistemas), desactivarla puede impedir nuevos accesos, pero no elimina los datos que el proveedor ya almacenaba ni los que el atacante hubiera obtenido. Tampoco acredita por sí sola que el riesgo haya cesado.

El establecimiento debe evaluar las consecuencias para las personas, documentar la brecha y realizar las comunicaciones a la Agencia Española de Protección de Datos y a los afectados conforme a la normativa. Si están enviándose mensajes fraudulentos a huéspedes, la advertencia preventiva no debería esperar al informe final.

3. El proveedor del motor de reservas ha sufrido una brecha, no se han filtrado datos de tarjetas y ya ha avisado a los huéspedes. ¿Debe hacer algo más el hotel?

Sí. La ausencia de datos de tarjeta no elimina el riesgo, especialmente si los nombres y detalles de las reservas se están utilizando para suplantar al hotel y engañar a sus clientes. Cuando el proveedor trata esos datos por cuenta del establecimiento, este sigue teniendo que documentar la brecha, evaluar sus riesgos y comprobar que se cumplen las obligaciones de comunicación.

Eso no significa que deba enviar un segundo aviso idéntico. La comunicación del proveedor puede ser suficiente si estaba autorizado para realizarla por cuenta del hotel, llegó a los huéspedes afectados y explicó el incidente, sus posibles consecuencias, las medidas adoptadas

y un contacto de ayuda. El hotel debe revisar el mensaje y las evidencias de envío y completarlo si faltan información o recomendaciones necesarias para que los huéspedes puedan protegerse.

Lo que ese aviso no sustituye es la notificación a la AEPD cuando resulte exigible. Si el proveedor afirma haberla presentado, el hotel debe obtener copia y justificante y comprobar que estaba facultado para actuar en su nombre y que la notificación comprendía el tratamiento afectado del establecimiento. Una notificación referida únicamente a los tratamientos propios del proveedor no cubre automáticamente al hotel.

4.- ¿Debe el contrato con el proveedor del PMS o del motor de reservas prever cómo actuar ante una brecha de seguridad?

Sí. Cuando el proveedor trata datos personales por cuenta del hotel, no basta con que el contrato indique que cumplirá el RGPD. El acuerdo de encargo debe recoger las obligaciones exigidas por el artículo 28, incluidas las medidas de seguridad y la asistencia al establecimiento. Para facilitar la respuesta ante una brecha, conviene concretar quién recibirá el aviso, por qué canal, qué información deberá facilitarse y cómo colaborará el proveedor en la investigación y conservación de evidencias.

Esta regulación debe permitir que el hotel actúe a tiempo. El proveedor debe comunicar la brecha sin dilación indebida desde que tenga conocimiento de ella, sin esperar al informe técnico definitivo ni a completar la evaluación del riesgo. No dispone de un plazo general propio de 72 horas para avisar al hotel. Pueden pactarse plazos operativos más concretos y actualizaciones sucesivas, pero sin rebajar esa exigencia legal.

El contrato también debe garantizar que el hotel pueda comprobar el cumplimiento del proveedor mediante información y auditorías: no se trata de una concesión voluntaria, sino de una obligación prevista en el RGPD. Asimismo, debe precisarse si el proveedor está autorizado para realizar notificaciones o comunicaciones por cuenta del establecimiento. Todo ello debe coordinarse con el contrato principal y sus condiciones de asistencia, responsabilidad y seguros, sin que lo pactado pueda limitar los derechos de los afectados ni las facultades de la autoridad de control.

5. El hotel ya ha advertido a los huéspedes que recibieron mensajes fraudulentos. ¿Es suficiente o debe completar el aviso e informar a otras personas antes de recibir el informe técnico definitivo?

Lo importante es qué información recibieron los huéspedes, no que el aviso se denominara “comunicación formal”. Una respuesta individual puede cumplir el artículo 34 del RGPD si explica la brecha, sus posibles consecuencias, las medidas adoptadas y un punto de contacto. En cambio, limitarse a confirmar que un WhatsApp no procede del hotel sirve para frenar el engaño, pero generalmente no basta para cumplir esa obligación.

En el supuesto consultado, los mensajes utilizaban información real de las reservas y algunos huéspedes llegaron a facilitar datos de pago. Estos hechos justifican gestionar la comunicación como un supuesto de probable alto riesgo, salvo evidencias concretas que permitan otra

valoración. Por ello, si el aviso inicial era insuficiente, debe completarse sin esperar al informe definitivo, explicando lo que se conoce y aclarando qué aspectos siguen investigándose. La finalidad es que los afectados puedan protegerse mientras persiste el riesgo.

El mensaje debe ofrecer recomendaciones concretas: no seguir enlaces sospechosos, comprobar las solicitudes directamente con el establecimiento y contactar inmediatamente con el banco si se facilitaron datos de pago. También debe distinguir entre la información expuesta en la brecha y la que los huéspedes entregaron posteriormente a los estafadores, sin presentar como confirmado lo que todavía se desconoce.

La actuación tampoco debe limitarse a quienes hayan contactado con el hotel. Debe extenderse a los demás huéspedes comprendidos en el ámbito razonablemente afectado para los que sea probable un alto riesgo, aunque aún no hayan comunicado ningún intento de fraude. Los avisos deben enviarse por canales seguros, sin revelar los destinatarios entre sí y conservando constancia de su contenido y envío.

6. Si el proveedor no puede identificar qué reservas fueron consultadas o extraídas, ¿a qué huéspedes debe informar el hotel?

La comunicación no debe limitarse a quienes hayan alertado del fraude, pero tampoco extenderse sin criterio a toda la clientela. El hotel debe determinar, con la información disponible, qué huéspedes pudieron verse afectados y para cuáles es probable que exista un alto riesgo. Tanto esa valoración como las incertidumbres que impidan precisar el alcance deben quedar documentadas.

Para concretar ese grupo, hay que reconstruir qué datos recibía y conservaba el proveedor, qué reservas eran accesibles desde los sistemas comprometidos y durante qué periodo. Lo relevante no es únicamente la fecha de estancia, sino si los datos estaban disponibles para el atacante. Así, una reserva antigua puede estar afectada si seguía almacenada. Por la misma razón, desconectar la integración con el proveedor no permite descartar la exposición de los datos que este ya conservaba.

Si la información disponible no permite acotar justificadamente ese grupo, será razonable ampliar la advertencia a los huéspedes cuyos datos pudieron estar accesibles y para los que sea probable un alto riesgo. En ese caso, debe explicarse que la afectación es potencial y que la investigación continúa: la falta de registros no demuestra que no hubiera acceso, pero tampoco permite afirmar que se extrajera toda la base de datos.

Siempre que sea viable, el aviso debe dirigirse individualmente a los afectados. Sustituirlo por una comunicación pública exige justificar que el contacto individual supone un esfuerzo desproporcionado y adoptar una medida que los informes de manera igualmente efectiva; el mero hecho de que existan muchos destinatarios no basta para prescindir del aviso directo.

7. Si los huéspedes están recibiendo mensajes fraudulentos, ¿puede el hotel avisarles antes de notificar la brecha a la AEPD? ¿Ese aviso sustituye a la notificación?

El hotel puede avisar a los huéspedes antes de notificar a la AEPD, pero ese aviso no sustituye la notificación cuando sea obligatoria. Si están recibiendo solicitudes fraudulentas de pago, no

debe retrasarse una advertencia que pueda evitarles un perjuicio mientras se prepara la comunicación a la Agencia. La comunicación exigida por el artículo 34 del RGPD debe realizarse sin dilación indebida: no dispone de un plazo propio de 72 horas.

Se trata de dos obligaciones distintas que pueden atenderse en paralelo. La brecha debe notificarse a la autoridad salvo que sea improbable que genere un riesgo para los derechos y libertades de las personas. Si, además, es probable que entrañe un alto riesgo, debe comunicarse también a los afectados, salvo que concurra alguna de las excepciones legales. Avisar primero a los clientes no permite retrasar ni omitir la notificación a la AEPD.

Distinto es enviar una advertencia preventiva sobre intentos de fraude cuando todavía no se ha identificado una brecha de datos personales. Ese aviso puede ser conveniente para proteger a los huéspedes y no activa, por sí solo, la obligación de notificar a la Agencia. Lo determinante sigue siendo comprobar si existe una brecha y evaluar el riesgo que supone.

Por último, las excepciones a la comunicación individual deben justificarse, no presumirse. Por ejemplo, no basta con que el sistema utilizara cifrado si el atacante pudo leer los datos mediante credenciales comprometidas, ni cambiar las contraseñas elimina el riesgo derivado de información que ya hubiera copiado. Para prescindir de esa comunicación, el hotel debe acreditar que se cumplen las condiciones de la excepción aplicable y dejar constancia de ello en el expediente.

8. Si el establecimiento todavía espera el informe técnico y desconoce el alcance completo de la brecha, ¿cuándo empiezan las 72 horas para notificarla?

El plazo comienza cuando el hotel tiene un grado razonable de certeza de que se han comprometido datos personales, no cuando recibe el informe técnico definitivo. Una sospecha puede requerir una comprobación inicial breve, pero esta debe iniciarse de inmediato y no utilizarse para retrasar el reconocimiento de una brecha que ya está suficientemente constatada.

Desde ese momento, el hotel debe notificar a la AEPD sin dilación indebida y, de ser posible, dentro de las 72 horas siguientes, salvo que sea improbable que la brecha genere un riesgo para los derechos y libertades de las personas. El cómputo incluye fines de semana y festivos: no se trata de tres días hábiles.

Si todavía se desconoce el número exacto de afectados o la causa del incidente, debe presentarse la información disponible, aclarando qué datos son provisionales y qué aspectos siguen investigándose, y completarla posteriormente sin dilación indebida. Por tanto, la falta de respuesta del proveedor no suspende el plazo ni la llegada de un informe posterior lo reinicia.

Si las 72 horas ya han transcurrido y la notificación era obligatoria, debe realizarse sin más demora e indicar los motivos del retraso, aunque explicarlos no garantiza que se considere justificado. En todo caso, el expediente debe recoger cuándo se tuvo constancia de la brecha, las actuaciones realizadas y la valoración que motivó la decisión de notificar o, cuando proceda, de no hacerlo.

9. La AEPD ya ha registrado la notificación de la brecha. ¿Cuándo debe ampliarse y qué debe indicarse si el proveedor todavía no facilita toda la información?

El registro acredita que la notificación se ha presentado, pero no significa que la AEPD dé por cerrado el incidente ni considere correcta su gestión. El hotel debe completar la información sin dilación indebida conforme conozca datos relevantes sobre el alcance de la brecha, sus consecuencias o las actuaciones realizadas, y atender los requerimientos que reciba de la Agencia.

Por ejemplo, habrá que actualizar la notificación si se identifican más afectados, nuevos tipos de datos comprometidos o un periodo de exposición diferente. También si se confirma que la información está utilizándose para enviar mensajes fraudulentos o que algunos huéspedes han facilitado datos de pago. En este último caso, debe distinguirse entre los datos expuestos en la brecha inicial y los obtenidos posteriormente mediante el engaño, sin atribuir a la filtración información cuya extracción no esté acreditada.

Si el proveedor sigue sin entregar los registros o el informe técnico, el hotel debe explicar qué información falta, qué gestiones ha realizado para obtenerla y qué medidas está adoptando mientras tanto. La actualización debe reflejar lo que se conoce y lo que continúa pendiente, sin esperar indefinidamente al proveedor ni presentar como confirmadas meras estimaciones.

Estas aportaciones deben vincularse a la notificación inicial mediante los cauces habilitados por la AEPD. Su guía contempla, con carácter general, completar la notificación inicial mediante una modificación dentro de los 30 días hábiles siguientes a su presentación. No obstante, ese plazo operativo no permite reservar información relevante hasta el último día: el artículo 33.4 del RGPD exige facilitarla progresivamente sin dilación indebida.

10. ¿Notificar una brecha a la AEPD supone que se abrirá un procedimiento sancionador contra el hotel?

No. Notificar una brecha es cumplir una obligación legal, no reconocer que el hotel ha cometido una infracción. La notificación no provoca automáticamente un procedimiento sancionador, aunque la AEPD puede solicitar aclaraciones o investigar si aprecia indicios de incumplimiento. Por tanto, comunicar lo ocurrido tampoco excluye las posibles responsabilidades derivadas de deficiencias en la seguridad o en la gestión del incidente.

La prudencia debe centrarse en informar con precisión, diferenciando los hechos confirmados de los aspectos que siguen investigándose y evitando atribuir responsabilidades a un proveedor sin evidencias suficientes. No consiste en ocultar el incidente o retrasar una notificación obligatoria por temor a que la Agencia examine lo sucedido.

La decisión de notificar depende del riesgo para las personas, no de la posibilidad de recibir una sanción. Si es improbable que la brecha genere un riesgo para sus derechos y

libertades, puede no notificarse, pero esa conclusión debe quedar razonada y documentada. Cuando la notificación sea exigible, realizarla diligentemente forma parte del cumplimiento; omitirla, retrasarla sin justificación o desatender los requerimientos de la AEPD puede añadir un incumplimiento a los que, en su caso, se detecten al investigar la brecha.

11. Si el proveedor del PMS o del motor de reservas no entrega los registros ni el informe técnico, ¿qué debe hacer el hotel?

Lo recomendable es enviar un requerimiento fehaciente, sin paralizar las medidas de protección de los huéspedes. Debe dirigirse al proveedor por el canal contractual, con constancia de recepción, y trasladarse a sus contactos de seguridad y protección de datos. Conviene exigir la conservación de las evidencias y una primera respuesta urgente, fijando un plazo concreto y proporcionado a la gravedad del incidente. Ese plazo no amplía los que deba cumplir el hotel para notificar o comunicar la brecha.

Para que el requerimiento resulte útil, debe precisar qué información se necesita: cronología, sistemas y cuentas comprometidos, datos potencialmente afectados, registros disponibles, intervención de subencargados y medidas adoptadas. No es necesario esperar al informe definitivo para exigir resultados provisionales. Si alguna información no existe o no puede facilitarse, debe solicitarse una explicación y las comprobaciones alternativas posibles. La petición debe limitarse a lo necesario para investigar el tratamiento afectado, evitando acceder injustificadamente a datos de otros clientes; pueden utilizarse extractos, acceso controlado o un auditor independiente.

En paralelo, cuando el proveedor actúe como encargado, el hotel puede ejercer los derechos de información y auditoría previstos en el artículo 28.3.h) del RGPD. Si persiste la falta de colaboración, conviene reflejarla en las ampliaciones de la notificación de la brecha y valorar un escrito específico ante la AEPD sobre los posibles incumplimientos del proveedor. No es obligatorio agotar una secuencia rígida ni terminar la auditoría antes de informar a la Agencia.

Mientras tanto, deberán valorarse las medidas necesarias para contener el incidente, incluida la suspensión de accesos cuando proceda, y las acciones contractuales frente al proveedor. La intervención de la AEPD permite investigar posibles incumplimientos de protección de datos, pero no sustituye una reclamación económica. Por tanto, exigir responsabilidades al proveedor y cumplir las obligaciones propias del hotel son actuaciones que deben avanzar de forma coordinada, sin que una quede pendiente de la otra.

12. Si el proveedor todavía no ha entregado el informe definitivo, ¿qué debe conservar el hotel para acreditar que ha actuado diligentemente?

El establecimiento debe poder demostrar qué medidas tenía implantadas antes del incidente y cómo reaccionó al conocerlo, aunque la investigación siga abierta. Para ello, el expediente debe recoger cuándo tuvo constancia de la brecha, qué información conocía en cada momento, cómo fue valorando el riesgo y qué medidas adoptó. También deben constar quién

tomó las decisiones y las comunicaciones realizadas a la AEPD y a los huéspedes, incluidas las evidencias de envío y las razones para informar a determinados grupos de reservas o excluirlos.

Ese relato debe apoyarse en la documentación disponible: contratos con los proveedores, garantías de seguridad exigidas, formación del personal y revisiones de accesos, junto con los requerimientos de información, sus justificantes de recepción, las respuestas obtenidas y las actuaciones de auditoría. Así podrá comprobarse tanto la preparación previa del establecimiento como su esfuerzo por esclarecer y gestionar lo ocurrido.

Si el informe definitivo no llega, puede elaborarse un informe provisional, diferenciando los hechos acreditados, las hipótesis y su fundamento, las limitaciones de la investigación y las actuaciones pendientes. Lo importante es reflejar fielmente lo que se sabe y lo que se ha hecho, sin presentar como confirmados datos desconocidos ni dar por realizadas comprobaciones que no se efectuaron. El expediente y sus evidencias deben custodiarse con acceso limitado y conservarse durante un tiempo proporcionado a sus finalidades.

En definitiva, acreditar que se ha requerido información al proveedor es importante, pero no sustituye las medidas que el propio establecimiento podía adoptar para proteger a los huéspedes mientras esperaba su respuesta.

13. Si el proveedor no conserva registros que permitan investigar la brecha, ¿puede exigírsele responsabilidad?

Sí, si esa carencia supone un incumplimiento de sus obligaciones de seguridad o de los compromisos asumidos con el hotel. La ausencia de un determinado registro no basta, por sí sola, para concluir que existe responsabilidad: el RGPD no establece los mismos registros ni plazos de conservación para todos los sistemas. Habrá que comprobar qué información debía conservar el proveedor atendiendo al servicio, a los riesgos y a lo pactado contractualmente.

Por ello, no disponer de registros que resultaban exigibles, eliminarlos indebidamente tras conocer el incidente o negarse sin justificación a facilitar información o colaborar en una auditoría puede constituir un incumplimiento. Que la investigación siga abierta no permite dejar al hotel sin información: el informe definitivo puede requerir tiempo, pero el proveedor debe comunicar los hechos conocidos y aportar las actualizaciones necesarias para gestionar la brecha.

Si se acredita ese incumplimiento, pueden derivarse consecuencias administrativas y contractuales. Para reclamar una indemnización al proveedor, el hotel deberá acreditar además los daños o costes sufridos y su relación con el incumplimiento; no basta con que la investigación haya resultado difícil o incompleta. Esa posible responsabilidad del proveedor tampoco exime de examinar si el establecimiento cumplió sus propias obligaciones de prevención y respuesta al incidente. Cada parte deberá responder por los

incumplimientos que le sean atribuibles, sin trasladar automáticamente al otro todas las consecuencias.

14. Si los huéspedes reciben mensajes fraudulentos que utilizan datos de reservas comercializadas a través de una OTA, ¿qué debe hacer el hotel?

No debe darse por hecho que la brecha se ha producido en la OTA. La información podría haberse obtenido de la plataforma, de la cuenta del hotel en la extranet o de un proveedor conectado. Es necesario comprobar el origen y solicitar información escrita a la OTA, sin retrasar las medidas de protección mientras se investiga.

Esta comprobación permite determinar qué obligaciones corresponden a cada parte. Las condiciones públicas de las OTAS suelen establecer que la plataforma y el hotel actúan como responsables independientes de sus respectivos tratamientos. No obstante, debe revisarse el contrato aplicable y las funciones reales de cada uno, pues una actuación conjunta podría exigir analizar una posible corresponsabilidad.

Si se confirma que la brecha afecta exclusivamente al tratamiento de la OTA corresponderá esta realizar las notificaciones y comunicaciones legalmente exigibles ante su autoridad competente y las personas afectadas. El hotel no debe duplicar automáticamente esa notificación como si hubiera sufrido una brecha propia. En cambio, si también se han comprometido datos bajo su responsabilidad, deberá evaluar el riesgo, documentar lo ocurrido y cumplir las obligaciones que le correspondan, aunque la OTA esté gestionando sus propias actuaciones.

En cualquier caso, conviene conservar los mensajes fraudulentos, asegurar las cuentas y coordinar las advertencias a los huéspedes.

15. Si los huéspedes reciben mensajes de WhatsApp que suplantán al hotel y les solicitan pagos, ¿puede responder el establecimiento por el dinero perdido?

La utilización fraudulenta del nombre del hotel no genera, por sí sola, responsabilidad para el establecimiento. Habrá que comprobar cómo se obtuvieron los datos, qué obligaciones correspondían a cada parte y si algún incumplimiento contribuyó al perjuicio. También serán relevantes la apariencia del mensaje y la reacción del hotel al conocer el fraude. Que la reserva proceda de una plataforma no demuestra que la información se haya obtenido de sus sistemas.

Ahora bien, el hotel no debe esperar a que se determine la responsabilidad para proteger a sus huéspedes. Debe adoptar medidas razonables: advertir a quienes estén en riesgo, aclarar sus canales legítimos de pago, revisar sus accesos y comunicar la incidencia a los proveedores o plataformas implicados. Si el origen sigue investigándose, debe explicarlo sin atribuir el ataque a terceros. A quienes hayan facilitado datos de pago se les recomendará contactar inmediatamente con su banco.

Cuando intervenga una OTA, deberán revisarse también las condiciones aplicables sobre coordinación de comunicaciones. Estas no pueden impedir el cumplimiento de las obligaciones legales de protección de datos. Además, debe distinguirse entre una advertencia preventiva para frenar el fraude y la comunicación de una brecha exigida por el RGPD: pueden coordinarse, pero un aviso genérico no sustituye una comunicación legalmente obligatoria si no reúne su contenido.

Si el huésped reclama una indemnización, será necesario analizar el daño y su relación con un incumplimiento atribuible al hotel. No procede asumir un reembolso automático ni rechazar la reclamación sin examinar lo sucedido. Conservar las evidencias y documentar la respuesta permitirá defender la actuación del establecimiento y valorar las reclamaciones frente a proveedores, plataformas o entidades financieras, así como las coberturas del seguro que puedan resultar aplicables.

16. ¿Quién debe cumplir PSD2: el establecimiento, la OTA, el proveedor tecnológico o el banco?

La obligación regulatoria de aplicar autenticación reforzada de clientes corresponde a los proveedores de servicios de pago que intervienen. El artículo 68 del Real Decreto-ley 19/2018 la exige en los supuestos previstos, entre ellos la iniciación de pagos electrónicos, con el régimen técnico y las excepciones aplicables. En un pago con tarjeta intervienen, entre otros, el emisor y el adquirente. El hotel no adquiere esa condición por aceptar pagos y un motor de reservas tampoco por prestar únicamente un servicio técnico.

La autenticación reforzada, conocida como SCA, exige factores independientes de categorías distintas: algo que el usuario conoce, posee o le es inherente. No debe confundirse con tener dos contraseñas ni con el doble factor utilizado para acceder al PMS o al correo, que pertenece a la seguridad de esos sistemas.

El establecimiento debe organizar el cobro con su adquirente, pasarela y, cuando intervenga, la OTA, de modo que pueda aplicarse SCA cuando corresponda y quede clara la función de cada uno. No debe reconvertir artificialmente una operación en telefónica o iniciada por el comercio para evitar la autenticación. Las exenciones o exclusiones dependen de la operación y de los requisitos aplicables, no de una elección libre del establecimiento.

En reservas garantizadas y cargos posteriores, incluidas determinadas cancelaciones o no presentaciones, puede existir una operación iniciada exclusivamente por el hotel sobre la base de un mandato válido del huésped. La EBA (Autoridad Bancaria Europea, por sus siglas en inglés) aclara que el mandato otorgado por un canal remoto debe establecerse con SCA en el supuesto analizado; los cargos posteriores deben ajustarse a sus condiciones. Una OTA puede obtener ese mandato por cuenta del hotel si existe la relación contractual adecuada y se identifica al beneficiario. Disponer del número de tarjeta no equivale, por sí solo, a tener autorización para cualquier cargo.

Esta nota interna es de uso interno exclusivo de clientes T&L, sin que pueda reproducirse, publicarse o divulgarse a terceros sin el consentimiento expresa de T&L.