

¿QUÉ HACER SI UN HOTEL SUFRE UN PHISHING? RESPONSABILIDAD, FRAUDE Y BRECHAS DE DATOS



Tourism & Law

Legal experts in travel business

Organizado para:



CEHAT

CONFEDERACIÓN ESPAÑOLA DE HOTELES
Y ALOJAMIENTOS TURÍSTICOS



Lo que vamos a ver

1. EL PHISHING COMO RIESGO PARA EL HOTEL

- 1.1. QUÉ ES EL PHISHING Y CÓMO HA EVOLUCIONADO
- 1.2. PRINCIPALES MODALIDADES DE FRAUDE Y SUPLANTACIÓN
- 1.3. RIESGOS ESPECÍFICOS PARA LOS ESTABLECIMIENTOS HOTELEROS
- 1.4. CASO PRÁCTICO: CAMBIO FRAUDULENTO DE CUENTA BANCARIA



2. RESPONSABILIDAD DEL ESTABLECIMIENTO

- 2.1. ¿QUIÉN RESPONDE CUANDO SE PRODUCE EL FRAUDE?
- 2.2. HOTEL, PROVEEDOR, CLIENTE Y ENTIDAD BANCARIA
- 2.3. RESPONSABILIDAD DE LOS PROVEEDORES TECNOLÓGICOS
- 2.4. CÓMO ACREDITAR LA DILIGENCIA DEL HOTEL



3. PREVENCIÓN Y REDUCCIÓN DEL RIESGO

- 3.1. PERSONAS, PROCESOS Y TECNOLOGÍA
- 3.2. PROTOCOLOS DE PAGOS Y VERIFICACIÓN
- 3.3. CONTRATOS CON PROVEEDORES TECNOLÓGICOS
- 3.4. CIBERSEGURO, FRAUDE E INGENIERÍA SOCIAL



Lo que vamos a ver

4. BRECHAS DE SEGURIDAD Y PROTECCIÓN DE DATOS

- 4.1. CUÁNDO UN PHISHING SE CONVIERTE EN UNA BRECHA
- 4.2. QUÉ DATOS Y SISTEMAS PUEDEN ESTAR AFECTADOS
- 4.3. EVALUACIÓN DEL RIESGO PARA LAS PERSONAS
- 4.4. NOTIFICACIÓN A LA AEPD: PLAZO DE 72 HORAS
- 4.5. COMUNICACIÓN A LAS PERSONAS AFECTADAS
- 4.6. DOCUMENTACIÓN Y RESPONSABILIDAD PROACTIVA



5. CÓMO ACTUAR CUANDO OCURRE

- 5.1. LAS PRIMERAS HORAS: CONTENER Y PRESERVAR EVIDENCIAS
- 5.2. BANCO, PROVEEDOR TECNOLÓGICO, ASEGURADORA E INCIBE
- 5.3. DENUNCIA Y GESTIÓN INTERNA DEL INCIDENTE
- 5.4. QUÉ DEBE TENER PREPARADO EL ESTABLECIMIENTO
- 5.5. CHECKLIST FINAL Y CONCLUSIONES



6. CONCLUSIONES

1. EL PHISHING COMO RIESGO PARA EL HOTEL



1.1. Qué es el phishing y cómo ha evolucionado



- o **Técnica de engaño basada en la suplantación de identidad** para obtener credenciales, pagos, datos o acceso a sistemas.
- o **Ya no se limita al correo mal redactado:** hoy puede llegar por email, SMS, WhatsApp, llamada o herramientas corporativas.
- o **El atacante utiliza relaciones de confianza:** proveedores, directivos, plataformas, bancos o incluso clientes.
- o **Su objetivo es inducir una acción concreta:** pulsar un enlace, descargar un archivo, facilitar claves o realizar una transferencia.
- o **El problema no es solo tecnológico:** puede generar consecuencias económicas, contractuales, reputacionales y de protección de datos.



1.2. Principales modalidades de fraude y suplantación

- o **Phishing:** correo electrónico que suplanta a una entidad o persona legítima.
- o **Smishing y vishing:** fraude mediante SMS, mensajería o llamada telefónica.
- o **Fraude del CEO o del directivo:** orden falsa de pago o petición urgente de información sensible.
- o **Cambio fraudulento de cuenta bancaria:** se comunica un nuevo IBAN aparentemente legítimo para desviar pagos.
- o **Suplantación frente al cliente:** envío de enlaces de pago falsos aparentando proceder del hotel.
- o **Compromiso de cuentas corporativas:** uso de correos o sistemas reales del establecimiento para reforzar la apariencia de autenticidad.

1. EL PHISHING COMO RIESGO PARA EL HOTEL



1.3. Riesgos específicos para los establecimientos hoteleros



- o **Alta exposición operativa:** pagos frecuentes, reservas, cancelaciones, reembolsos y comunicaciones constantes con terceros.
- o **Concurrencia de múltiples interlocutores:** clientes, OTAs, proveedores, bancos, directivos, recepción y administración.
- o **Gestión de información especialmente sensible:** datos identificativos, reservas, facturación, documentación y, en ocasiones, datos bancarios.
- o **Entornos de urgencia y presión operativa** que favorecen errores de verificación.
- o **Posible afectación a varios planos a la vez:** pérdida económica, interrupción operativa, reclamaciones de terceros y brecha de datos personales.

1.4. Caso práctico: cambio fraudulento de cuenta bancaria



- o El hotel recibe un correo **aparentemente enviado por un proveedor habitual** comunicando un cambio de IBAN.
- o El mensaje utiliza **datos reales, firma habitual y contexto auténtico**, por lo que resulta verosímil.
- o El establecimiento realiza la transferencia y, días después, **el proveedor legítimo reclama el pago**.
- o El incidente plantea varias cuestiones:
 - o ¿Quién soporta la pérdida económica?
 - o ¿Sigue pendiente la deuda con el proveedor real?
 - o ¿Actuó diligentemente el hotel?
 - o ¿Hay implicaciones para el banco, el proveedor tecnológico o la aseguradora?
- o Si además el atacante accedió al correo o a sistemas del hotel, **puede existir también una brecha de seguridad de datos personales**.

2. RESPONSABILIDAD DEL ESTABLECIMIENTO



2.1. ¿Quién responde cuando se produce el fraude?



- o Que el hotel sea víctima de una estafa no determina por sí solo quién debe soportar el perjuicio.
- o Es necesario reconstruir cómo se produjo el fraude y qué actuación tuvo cada interviniente.
- o Deben analizarse las obligaciones contractuales, las medidas de seguridad existentes y la diligencia desplegada.
- o Una cuestión central será determinar si existían señales que exigían una comprobación adicional antes de realizar la operación.
- o La existencia de un delito cometido por un tercero no excluye automáticamente posibles responsabilidades civiles o contractuales.

2.2. Hotel, proveedor, cliente y entidad bancaria



- o **Hotel:** puede responder si una actuación negligente o una deficiencia de sus controles contribuye al perjuicio.
- o **Proveedor:** habrá que valorar si su correo o sistemas estaban comprometidos y qué medidas de seguridad había adoptado.
- o **Cliente:** puede resultar perjudicado si recibe desde un entorno aparentemente legítimo un falso enlace o solicitud de pago.
- o **Entidad bancaria:** debe distinguirse entre una operación no autorizada y una transferencia que el empleado autoriza engañado.
- o En **pagos fraudulentos**, la actuación debe ser inmediata: comunicar el fraude al banco e intentar recuperar los fondos, sin asumir que la devolución sea automática.

2. RESPONSABILIDAD DEL ESTABLECIMIENTO

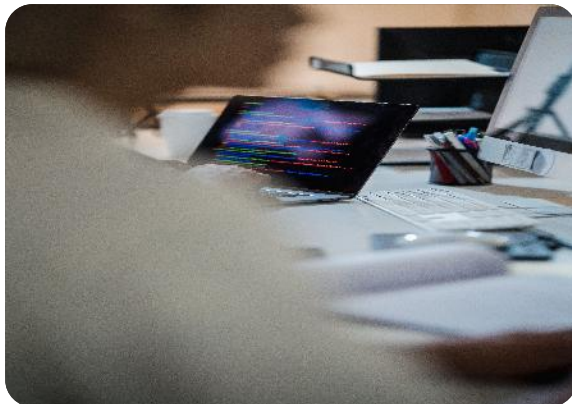


2.3. Responsabilidad de los proveedores tecnológicos



- o Externalizar un servicio tecnológico no traslada automáticamente toda la responsabilidad al proveedor.
- o Debe analizarse qué servicio tenía contratado el hotel y qué obligaciones asumía cada parte.
- o Importa determinar quién gestionaba actualizaciones, accesos, credenciales, copias de seguridad y monitorización.
- o Si el proveedor detecta un incidente, resulta esencial cuándo lo comunica y qué asistencia presta para contenerlo e investigarlo.
- o Si además actúa como encargado del tratamiento, tendrá obligaciones específicas conforme al RGPD.

2.4. Cómo acreditar la diligencia del hotel



- o Disponer de protocolos internos conocidos y documentados, especialmente para pagos y cambios de cuentas bancarias.
- o Implantar doble verificación y, cuando proceda, doble autorización en operaciones sensibles.
- o Mantener formación periódica y documentada del personal.
- o Aplicar medidas técnicas adecuadas: Control de accesos, actualizaciones, registros y copias de seguridad.
- o Conservar evidencias de todo ello: procedimientos, formación, contratos, análisis de riesgos, controles e incidencias.

3. PREVENCIÓN Y REDUCCIÓN DEL RIESGO



3.1. Personas, procesos y tecnología



- o La prevención eficaz debe apoyarse en tres pilares complementarios.
- o Personas: formación y capacidad para identificar y detener operaciones sospechosas.
- o Procesos: procedimientos claros para pagos, cambios bancarios, accesos y gestión de incidencias.
- o Tecnología: control de accesos, actualizaciones, registros, copias de seguridad y protección del correo.
- o El objetivo no es eliminar todo riesgo, sino reducirlo y poder acreditar que se adoptaron medidas proporcionadas.



3.2. Protocolos de pagos y verificación

- o Nunca cambiar un IBAN únicamente por una petición recibida por correo electrónico.
- o Verificar siempre mediante un segundo canal independiente y previamente conocido.
- o Para pagos relevantes, establecer doble autorización o controles reforzados.
- o No utilizar como referencia los datos de contacto incluidos en el propio mensaje sospechoso.
- o La urgencia no debe desactivar el control: es precisamente una de las técnicas más utilizadas por el atacante.

3. PREVENCIÓN Y REDUCCIÓN DEL RIESGO



3.3. Contratos con proveedores tecnológicos



- o El contrato debe definir qué servicio presta el proveedor y qué obligaciones asume cada parte.
- o Revisar responsabilidades sobre actualizaciones, accesos, copias, monitorización y seguridad.
- o Establecer cómo debe actuar el proveedor si detecta un incidente o una brecha.
- o Prever canales y tiempos de comunicación, colaboración en la investigación y conservación de evidencias.
- o Cuando trate datos personales por cuenta del hotel, revisar también el contrato de encargado del tratamiento.



3.4. Ciberseguro, fraude e ingeniería social

- o Tener un seguro cyber no significa que todo fraude esté cubierto.
- o Hay que distinguir entre ciberincidente, fraude, ingeniería social y transferencia autorizada bajo engaño.
- o Revisar límites, sublímites, franquicias y exclusiones.
- o Comprobar qué medidas de seguridad exige la aseguradora como condición de cobertura.
- o Conocer de antemano cómo y en qué plazo debe comunicarse el siniestro.

4. BRECHAS DE SEGURIDAD Y PROTECCIÓN DE DATOS

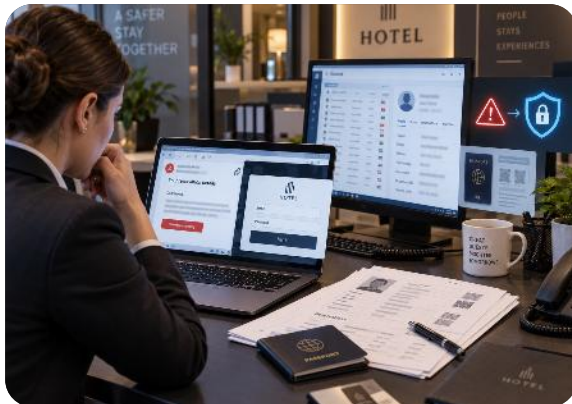


4.1. Cuándo un phishing se convierte en una brecha



- o No todo intento de phishing es una brecha de datos personales.
- o Existe brecha cuando el incidente provoca destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.
- o Si el empleado recibe el correo y no interactúa con él, normalmente estaremos ante un incidente de seguridad, no necesariamente ante una brecha.
- o Si entrega credenciales y el atacante accede al correo, PMS, CRM u otros sistemas, debe investigarse la posible afectación a datos personales.
- o La brecha puede afectar a la confidencialidad, integridad o disponibilidad de la información.

4.2. Qué datos y sistemas pueden estar afectados



- o Identificar qué cuentas, equipos y sistemas estuvieron accesibles y durante cuánto tiempo.
- o En un hotel pueden verse afectados correo corporativo, PMS, CRM, sistemas de reservas, facturación o recursos humanos.
- o Analizar qué información contenían: identificación, contactos, reservas, facturas y datos de empleados.
- o Prestar mayor atención a documentos de identidad, datos financieros o información especialmente sensible.
- o No basta con saber que hubo un acceso: hay que determinar qué información pudo realmente quedar expuesta.

4. BRECHAS DE SEGURIDAD Y PROTECCIÓN DE DATOS



4.3. Evaluación del riesgo para las personas



4.4. Notificación a la AEPD: plazo de 72 horas



- o Toda brecha exige valorar sus posibles consecuencias para los derechos y libertades de las personas.
- o Deben considerarse la naturaleza, sensibilidad y volumen de los datos afectados.
- o Analizar el número y características de las personas afectadas, incluida su posible vulnerabilidad.
- o Valorar consecuencias como fraude, suplantación de identidad, pérdida económica, daño reputacional o pérdida de confidencialidad.
- o También cuentan las medidas que reduzcan el riesgo: cifrado, bloqueo rápido, recuperación de credenciales o imposibilidad efectiva de utilización de los datos.

- o No toda brecha debe notificarse. La regla del RGPD es que deberá comunicarse a la AEPD salvo que sea improbable que la violación entrañe un riesgo para los derechos y libertades de las personas.
- o El análisis debe comenzar desde el momento en que existen indicios suficientes del incidente. Una vez que el hotel tiene constancia de que se ha producido una violación de datos personales, empieza a computarse el plazo de 72 horas.
- o La notificación debe realizarse sin dilación indebida y, cuando sea posible, dentro de esas 72 horas. No es un plazo para esperar ni para empezar a investigar al tercer día.
- o Antes de decidir, habrá que determinar, en la medida posible, qué ha ocurrido, qué sistemas y datos están afectados, a cuántas personas puede afectar y qué consecuencias previsibles puede generar.
- o La notificación a la AEPD debe describir, al menos, la naturaleza de la brecha, las categorías y número aproximado de afectados y registros, sus posibles consecuencias y las medidas adoptadas o previstas para contenerla y reducir sus efectos.
- o Si dentro de las 72 horas todavía no se dispone de toda la información, no es necesario esperar a cerrar la investigación: puede realizarse una primera notificación y completar posteriormente la información por fases.
- o Si la notificación se efectúa transcurridas las 72 horas, el responsable deberá explicar y justificar las razones del retraso.

4. BRECHAS DE SEGURIDAD Y PROTECCIÓN DE DATOS



4.5. Comunicación a las personas afectadas



- o La comunicación a los afectados tiene un umbral superior: procede cuando sea probable que la brecha entrañe un alto riesgo.
- o Debe realizarse sin dilación indebida y utilizando un lenguaje claro y comprensible.
- o Debe explicar, al menos, qué ha ocurrido, sus posibles consecuencias y qué medidas se han adoptado.
- o Debe facilitarse un punto de contacto y recomendaciones para que las personas puedan protegerse.
- o No toda brecha notificada a la AEPD exige automáticamente comunicarla a los afectados.

4.6. Documentación y responsabilidad proactiva



- o Toda brecha de datos personales debe quedar documentada, aunque finalmente no se notifique a la AEPD.
- o El expediente debe recoger hechos, cronología, datos afectados, consecuencias y medidas adoptadas.
- o Debe documentarse la evaluación del riesgo y la decisión de notificar o no notificar.
- o También deben conservarse evidencias técnicas, comunicaciones con proveedores y actuaciones correctivas.
- o El objetivo es poder demostrar que el hotel previno, reaccionó, evaluó y decidió de forma diligente.

5. CÓMO ACTUAR CUANDO OCURRE

5.1. Las primeras horas: contener y preservar evidencias



5.2. Banco, proveedor tecnológico, aseguradora



- o **Actuar inmediatamente:** no esperar a conocer todo el alcance del incidente para iniciar la respuesta.
- o **Detener y contener la actuación fraudulenta:** bloquear accesos, revocar sesiones, cambiar credenciales comprometidas y, cuando proceda, aislar los equipos afectados.
- o **No borrar ni alterar evidencias:** conservar correos, cabeceras, mensajes, archivos, URLs, capturas, registros de acceso y cualquier información relacionada con el ataque.
- o **Identificar** inicialmente qué cuentas, dispositivos o sistemas pueden estar comprometidos y desde cuándo.
- o **Activar la cadena interna de comunicación:** dirección, responsable técnico y, cuando pueda existir afectación a datos personales, asesor jurídico o DPD.
- o **Dejar constancia** desde el primer momento de qué ocurrió, cuándo se detectó y qué medidas se fueron adoptando.

- o **Banco:** si existe un pago o transferencia fraudulenta, contactar inmediatamente por los canales oficiales y solicitar la activación de las medidas antifraude y el intento de recuperación de los fondos.
- o **Proveedor tecnológico:** activar de inmediato al responsable del correo, PMS, CRM u otros sistemas afectados para contener el incidente, revisar accesos y preservar evidencias.
- o **Aseguradora:** comunicar el siniestro dentro de los plazos establecidos en la póliza y seguir las instrucciones previstas para activar las coberturas.
- o **INCIBE – 017:** puede prestar orientación y asistencia ante incidentes de ciberseguridad y ayudar a determinar las primeras actuaciones.
- o Estas comunicaciones deben realizarse en paralelo, no de forma sucesiva, porque el tiempo puede ser determinante.
- o Conservar siempre números de incidencia, comunicaciones, justificantes y respuestas recibidas.

5. CÓMO ACTUAR CUANDO OCURRE



5.3. Denuncia y gestión interna del incidente



5.4. Qué debe tener preparado el establecimiento



- o Valorar la denuncia ante Policía Nacional o Guardia Civil, aportando la información y evidencias disponibles: Unidad Central de Ciberdelincuencia (UCC).
- o La denuncia penal no sustituye las demás actuaciones: banco, aseguradora, proveedor tecnológico o protección de datos deben gestionarse por sus propios canales.
- o Abrir un expediente interno del incidente que permita reconstruir todo lo sucedido.
- o Documentar la cronología, sistemas afectados, comunicaciones realizadas, decisiones adoptadas y medidas de contención y recuperación.
- o Coordinar desde el inicio los planos técnico, jurídico, económico y de protección de datos.
- o Una vez controlado el incidente, analizar por qué ocurrió y qué medidas deben modificarse para reducir el riesgo de repetición

- o Una cadena de comunicación definida: quién recibe el aviso y quién toma las decisiones.
- o Un protocolo escrito de gestión de incidentes y brechas, conocido por quienes deben aplicarlo.
- o Un directorio actualizado de contactos críticos: proveedor tecnológico, banco, aseguradora, asesor jurídico/DPD e INCIBE.
- o Procedimientos específicos para pagos, cambios de IBAN y operaciones sensibles, con mecanismos de doble verificación.
- o Acceso rápido a la documentación necesaria: contratos tecnológicos, pólizas, encargos de tratamiento y procedimientos internos.
- o Capacidad para identificar qué sistemas contienen qué datos y qué proveedores tienen acceso a ellos.
- o Formación del personal para que todos conozcan una regla básica: si existe una sospecha, parar y comunicar inmediatamente.

6. CONCLUSIONES



1. El phishing no es solo un problema informático.

Puede convertirse simultáneamente en un problema económico, contractual, reputacional y de protección de datos.

2. La responsabilidad depende de cómo actuó cada parte.

Ser víctima de un fraude no determina automáticamente quién debe soportar el perjuicio. La diligencia, los controles y los contratos serán determinantes.

3. La mejor respuesta empieza antes del ataque.

Personas formadas, procedimientos claros, tecnología adecuada, contratos revisados y seguros correctamente dimensionados reducen tanto el riesgo como sus consecuencias.

4. Cuando ocurre, la rapidez es esencial.

Hay que contener, preservar evidencias, activar al banco y proveedores, comunicar el siniestro y analizar inmediatamente la posible afectación a datos personales.

5. En protección de datos hay que evaluar y documentar siempre.

No todo phishing es una brecha, no toda brecha se notifica y no toda brecha notificada exige informar a los afectados; pero toda brecha de datos personales debe gestionarse, valorarse y documentarse.

APÉNDICE: CHECK LIST



- ✓ ¿Tenemos formación periódica y documentada para el personal?
- ✓ ¿Utilizamos autenticación multifactor en los sistemas críticos?
- ✓ ¿Existe un procedimiento para cambios de IBAN y pagos sensibles?
- ✓ ¿Aplicamos doble verificación o doble autorización cuando el riesgo lo aconseja?
- ✓ ¿Tenemos correctamente gestionados los accesos, contraseñas, altas y bajas de usuarios?
- ✓ ¿Disponemos de copias de seguridad y registros de actividad suficientes?
- ✓ ¿Sabemos qué proveedores tecnológicos tienen acceso a nuestros sistemas y datos?
- ✓ ¿Están revisados los contratos, encargos de tratamiento y obligaciones de comunicación de incidentes?
- ✓ ¿Conocemos realmente qué cubren nuestras pólizas de ciberriesgo, fraude o ingeniería social?
- ✓ ¿Existe un protocolo de incidentes y brechas de datos personales conocido por quienes deben aplicarlo?
- ✓ ¿Tenemos identificados los contactos de emergencia: banco, proveedor tecnológico, aseguradora, asesor/DPD e INCIBE?
- ✓ ¿Podemos demostrar documentalmente todas estas medidas?



PREVENIR · DETECTAR · ACTUAR · DOCUMENTAR

La seguridad no consiste en garantizar que nunca habrá un incidente, sino en estar preparados para reducir su probabilidad, limitar sus consecuencias y poder demostrar que el establecimiento actuó con diligencia.





Tourism & Law

Legal experts in travel business

Gracias por tu atención

www.tourismandlaw.com