MANUAL DE CIBERSEGURIDAD para agencias de viajes

Guía práctica para prevenir, detectar y actuar ante ciberataques



Organiza:

AEVAV C.V.
ASOCIACIÓN EMPRESARIAL VALENCIANA DE AGENCIAS DE VIAJE

Con la colaboración de:

HISCOX

AON

LEY NET CONSULTORES

Elaborado a partir de la jornada organizada por AEVAV
Con la colaboración de AON, Hiscox y Leynet Consultores

Octubre 2026

soloAgentes
INFORMACIÓN Y FORMACIÓN PARA AGENTES DE VIAJES

Antes de empezar

La ciberseguridad de una agencia de viajes no depende únicamente del antivirus instalado en sus ordenadores.

Una agencia trabaja diariamente con correos electrónicos, reservas, proveedores, pagos, documentación de identidad, teléfonos móviles, aplicaciones de mensajería, plataformas de terceros, datos bancarios y, en ocasiones, información médica de sus clientes. Una incidencia en cualquiera de estos puntos puede provocar desde una interrupción temporal del trabajo hasta un fraude económico, una pérdida de información o una brecha de datos personales.

Este manual parte de una idea repetida durante la jornada organizada por AEVAV: la seguridad debe prepararse antes de que ocurra el incidente.

Como señaló Luis López Loma: «Lo primero y más fundamental es conocer toda tu infraestructura tecnológica.»

Las recomendaciones expuestas durante el seminario se han contrastado y complementado para este manual con documentación de la Agencia Española de Protección de Datos (AEPD) y del Instituto Nacional de Ciberseguridad (INCIBE).

El documento tiene una finalidad informativa y preventiva. Las circunstancias jurídicas, técnicas o aseguradoras de un incidente concreto pueden requerir la intervención de profesionales especializados.



MANUAL DE CIBERSEGURIDAD PARA AGENCIAS DE VIAJES

Guía práctica para prevenir, detectar y actuar ante ciberataques

Elaborado a partir de los contenidos, recomendaciones y casos prácticos abordados durante el Seminario de Ciberseguridad para Agencias de Viajes organizado por AEVAV, con la colaboración de Leynet , Hiscox y AON.

Con la participación de Luis López Loma, abogado especializado en derecho tecnológico; David Fernández Machi, Partnerships Manager de Hiscox; y Josep García González, responsable del área Travel de AON.

Jornada moderada por Miguel Ángel Domínguez García, abogado y gerente de AEVAV.

Octubre de 2026.



1. Saber qué tenemos antes de intentar protegerlo

El primer paso no consiste en comprar una nueva herramienta de seguridad.

Consiste en conocer qué sistemas, dispositivos, servicios y datos utiliza realmente la agencia.

En una pequeña empresa es frecuente que con el paso del tiempo se acumulen ordenadores antiguos, cuentas de correo, móviles, aplicaciones, accesos a plataformas, usuarios creados para antiguos empleados, discos USB o servicios contratados que nadie recuerda exactamente quién administra.

Todo aquello que existe y no está controlado puede convertirse en un punto de entrada.

La agencia debería poder responder con claridad a preguntas tan básicas como qué ordenadores y móviles se utilizan para trabajar; qué cuentas de correo existen; quién dispone de permisos de administrador; qué programas y plataformas de reservas se emplean; dónde se almacenan los documentos de clientes; qué sistemas contienen datos bancarios; qué servicios realizan copias de seguridad; quién puede acceder a ellos y qué debe ocurrir con los accesos cuando una persona deja de trabajar en la empresa.

El inventario no tiene que ser técnicamente complejo. Debe ser completo, actualizado y comprensible para la dirección de la agencia.



2. Las medidas básicas que deberían implantarse en cualquier agencia

Contraseñas diferentes y bien gestionadas

Utilizar una misma contraseña para distintos servicios multiplica las consecuencias de una filtración.

Si una contraseña comprometida permite acceder al correo electrónico y esa misma clave se utiliza en otras plataformas, un incidente aparentemente limitado puede propagarse rápidamente.

La recomendación es utilizar contraseñas únicas y suficientemente robustas y, cuando la cantidad de accesos haga difícil gestionarlas correctamente, emplear un gestor de contraseñas fiable.

No deben compartirse contraseñas por correo electrónico, mensajes de WhatsApp o documentos accesibles para toda la plantilla.

Activar el doble factor de autenticación

Siempre que el servicio lo permita, debe activarse un segundo factor de autenticación, especialmente en: correo electrónico, banca, herramientas de administración, almacenamiento en la nube, redes sociales corporativas y plataformas que contengan información relevante.

El doble factor añade una comprobación adicional a la contraseña y reduce considerablemente el riesgo de que unas credenciales robadas sean suficientes para acceder a una cuenta.

INCIBE recomienda expresamente el uso de doble factor y gestores de contraseñas como medidas básicas de seguridad empresarial.

Mantener los sistemas actualizados

Un ordenador puede funcionar aparentemente bien y, al mismo tiempo, mantener vulnerabilidades conocidas porque su sistema operativo o alguno de sus programas no se ha actualizado.

Deben mantenerse al día, entre otros elementos, los sistemas operativos, navegadores, aplicaciones, antivirus, programas de gestión, dispositivos de red y la web corporativa, incluidos su gestor de contenidos y complementos.

Una web abandonada durante años puede convertirse también en una puerta de entrada a la organización.

Limitar los permisos

No todas las personas necesitan tener acceso a todo.

El criterio debería ser sencillo: cada empleado dispone únicamente de los permisos que necesita para realizar su trabajo.

Las cuentas con permisos de administración deben utilizarse únicamente cuando resulte necesario y los accesos de antiguos empleados o colaboradores deben eliminarse cuando dejan de necesitarlos.



3. Las copias de seguridad no son opcionales

Uno de los mensajes más claros de la jornada fue la necesidad de disponer de copias de seguridad que permitan recuperar la actividad.

Una copia almacenada permanentemente en el mismo ordenador o en una unidad siempre conectada puede quedar cifrada junto con los archivos originales durante un ataque de ransomware.

Por eso no basta con decir «hacemos copias».

La agencia debe saber qué información se copia, con qué frecuencia, dónde se almacena y si realmente puede recuperarse
.
Una estrategia razonable para una pequeña agencia debería combinar copias automáticas frecuentes con una copia separada

del sistema principal y establecer comprobaciones periódicas para verificar que la restauración funciona. INCIBE recomienda realizar copias regularmente, conservarlas en entornos separados y comprobar que es posible recuperarlas.

La pregunta correcta no es «¿tenemos copia de seguridad?», sino:
Si mañana todos los ordenadores de la agencia dejaran de funcionar, ¿cuánto tardaríamos en volver a trabajar?



4. El correo electrónico: uno de los principales puntos de riesgo

Buena parte de los ataques no comienzan con una sofisticada intrusión técnica.

Empiezan con un correo. El phishing intenta que una persona haga aquello que el atacante necesita: abrir un archivo, introducir su contraseña, pulsar un enlace, descargar un programa o realizar un pago.

La inteligencia artificial ha mejorado además la calidad formal de muchos mensajes fraudulentos. La ausencia de faltas de ortografía ya no permite descartar que un correo sea falso.

Por eso hay que desconfiar especialmente cuando aparece alguno de estos elementos: urgencia inusual, cambios repentinos de procedimiento, solicitudes de credenciales, enlaces inesperados, documentos no solicitados, modificaciones de datos bancarios o mensajes que piden saltarse controles habituales.

Un correo puede parecer completamente normal y seguir siendo fraudulento.



5. El fraude del cambio de cuenta bancaria

Este fue uno de los riesgos que generó mayor debate durante la jornada porque afecta directamente a la operativa diaria de una agencia.

El esquema puede ser muy sencillo.

La agencia mantiene una conversación habitual con un proveedor. En algún momento recibe una factura o un mensaje aparentemente legítimo indicando que debe realizar el pago en una nueva cuenta bancaria.

La dirección desde la que llega el correo puede ser parecida a la original o incluso puede haberse comprometido una cuenta auténtica.

La agencia realiza la transferencia. Días después, el proveedor comunica que nunca recibió el dinero.

INCIBE identifica este ataque como Business Email Compromise (BEC) y describe precisamente supuestos en los que los delincuentes interceptan o suplantan comunicaciones de proveedores para sustituir la cuenta bancaria de una factura.

La norma operativa debería ser tajante: un cambio de cuenta bancaria nunca debe validarse únicamente mediante el mismo correo electrónico que comunica el cambio.

Debe comprobarse por un segundo canal independiente utilizando datos de contacto que la agencia ya conocía previamente.

Una llamada al teléfono habitual del proveedor puede evitar una pérdida de miles de euros.

También puede solicitarse un certificado de titularidad bancaria cuando proceda y extremar la comprobación en las altas de nuevos proveedores.

El procedimiento debe aplicarse incluso cuando el mensaje parezca proceder de una persona conocida.



6. Si ya hemos realizado una transferencia fraudulenta

La rapidez es fundamental.

En cuanto se detecte que se ha realizado un pago a una cuenta incorrecta o potencialmente fraudulenta, hay que ponerse inmediatamente en contacto con la entidad bancaria.

INCIBE recomienda comunicar el incidente al banco cuanto antes, ya que en determinados supuestos todavía puede ser posible intentar cancelar o bloquear una transferencia.

También recomienda reunir evidencias y presentar denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

No debe esperarse a «ver qué ocurre».

Deben conservarse correos, facturas, justificantes, mensajes, números de cuenta, cabeceras del correo y cualquier otra información relacionada con el fraude.



7. DNI, pasaportes y documentación de los clientes

Las agencias necesitan determinados datos para realizar reservas, emitir billetes o tramitar servicios, pero disponer de esos datos no autoriza a conservar indiscriminadamente cualquier documento.

El RGPD establece el principio de minimización: deben tratarse únicamente los datos necesarios para la finalidad concreta y limitar también el tiempo durante el cual permanecen accesibles.

Aquí conviene introducir una precisión importante respecto a una de las cuestiones comentadas durante el seminario.

No existe una regla general según la cual «nunca se pueda escanear un DNI».

Lo correcto es analizar si existe una necesidad y una base jurídica que justifiquen disponer de esa copia.

La AEPD señala que, con carácter general, no es necesario obtener una copia del DNI para realizar una contratación cuando la identidad puede verificarse por otros medios, salvo que exista una norma sectorial que exija expresamente esa copia.

La propia AEPD ha considerado excesiva, por ejemplo, la obtención de una copia completa del DNI o pasaporte para determinados procesos de check-in hotelero cuando se recaban más datos de los necesarios.

Por tanto, para una agencia la regla práctica debe ser: pedir solo aquello que realmente sea necesario y conservarlo únicamente durante el tiempo justificado.



8. Cuidado especial con los datos médicos

Una agencia puede terminar gestionando documentos que contienen información médica cuando un cliente necesita cancelar un viaje o justificar un siniestro ante una aseguradora.

Los datos relativos a la salud pertenecen a las denominadas categorías especiales de datos y reciben una protección reforzada en el RGPD.

Esto exige extremar el cuidado. La documentación no debería circular innecesariamente entre empleados ni mantenerse indefinidamente en bandejas de correo, teléfonos o carpetas accesibles para personas que no necesitan consultarla.

Cuando la agencia actúe simplemente como



9. WhatsApp no convierte un tratamiento de datos en ilegal, pero tampoco lo hace seguro por defecto

Durante la jornada surgió una situación muy habitual: un cliente envía la fotografía de su DNI, pasaporte o informe médico por WhatsApp.

La cuestión no debe resolverse con un simple «WhatsApp está permitido» o «WhatsApp está prohibido».

Cuando una empresa trata información de sus clientes sigue siendo responsable de aplicar las medidas de protección adecuadas. La AEPD recuerda que las entidades y profesionales pueden incurrir en responsabilidades cuando divulgan información privada de clientes mediante servicios de mensajería.

La agencia debería determinar de antemano qué documentación acepta por mensajería y qué debe suceder posteriormente con ella.

Hay que prestar especial atención a los respaldos automáticos del teléfono, las sesiones abiertas en ordenadores, los dispositivos personales, los grupos, la descarga automática de archivos y la permanencia innecesaria de documentos en el historial de conversaciones.

El criterio debe ser siempre el mismo: mínima información, mínimo acceso y mínimo tiempo de conservación compatible con la finalidad y las obligaciones legales de la agencia.



10. Qué es realmente una brecha de datos personales

No todo ciberataque es automáticamente una brecha que deba notificarse a la AEPD. Pero tampoco es necesario que los datos hayan sido publicados en Internet para que exista una brecha. La AEPD define una brecha de datos personales como un incidente que provoque destrucción, pérdida o alteración de información personal o un acceso o comunicación no autorizados. Puede producirse incluso por error y no necesariamente por un ataque. Por ejemplo, pueden constituir brechas: el acceso indebido a una base de datos, la pérdida de un dispositivo con información de clientes, el envío de documentación a un destinatario incorrecto, el borrado accidental de información o una intrusión.



11. Las 72 horas: qué significa realmente el plazo

Este es uno de los puntos que conviene dejar especialmente claro.

No existe una obligación de comunicar a la AEPD todos los incidentes informáticos en 72 horas.

La obligación se refiere a determinadas brechas de datos personales.

Cuando sea probable que una brecha suponga un riesgo para los derechos y libertades de las personas, el responsable debe notificarla a la autoridad de control sin dilación indebida y, cuando sea posible, dentro de las 72 horas desde que tiene constancia de ella.

Si además es probable que exista un alto riesgo para las personas afectadas, puede resultar necesario comunicarles directamente la brecha y explicarles qué ha ocurrido, qué consecuencias puede tener y qué medidas pueden adoptar.

Y aunque una brecha finalmente no tenga que notificarse, debe documentarse internamente de acuerdo con las obligaciones establecidas por el RGPD.

Por ello, una agencia no debería esperar al tercer día para empezar a estudiar el incidente.

Las 72 horas son un plazo máximo en determinados supuestos, no un plazo de reflexión.



12. Qué hacer cuando descubrimos un ciberataque

Un incidente genera presión y precisamente por eso es importante disponer de un procedimiento preparado.

Las primeras actuaciones deben buscar cuatro objetivos: contener el problema, conservar las evidencias, mantener o recuperar la actividad y determinar si existen obligaciones legales adicionales.

Hay que evitar que una persona, intentando «arreglar rápidamente el ordenador», elimine información que posteriormente resulte necesaria para saber qué ocurrió.

Dependiendo de la naturaleza del incidente, puede ser necesario desconectar equipos afectados de la red, bloquear cuentas, revocar sesiones, cambiar credenciales, avisar al proveedor tecnológico, contactar con especialistas en respuesta a incidentes, comunicarlo a la aseguradora y preservar los registros disponibles.

Si existen posibles consecuencias económicas o delictivas, deberán analizarse también las comunicaciones a las entidades financieras y Fuerzas y Cuerpos de Seguridad.

INCIBE recomienda preservar las evidencias relacionadas con un fraude antes de denunciarlo.



13. No destruir las pruebas intentando resolver el problema

Determinar quién sufrió realmente una intrusión puede ser decisivo en conflictos entre empresas.

En un fraude de cambio de cuenta bancaria, por ejemplo, puede ser necesario averiguar si el delincuente creó una dirección casi idéntica a la del proveedor, si comprometió el correo de la agencia o si accedió a la cuenta auténtica del proveedor.

Esto puede requerir analizar cabeceras de correo, registros de acceso, redirecciones, dispositivos y otros elementos técnicos.

Por eso se insistió durante el seminario en la necesidad de recurrir a profesionales capaces de realizar un análisis forense cuando la gravedad del caso lo requiera.

No conviene borrar, formatear o reinstalar precipitadamente el sistema antes de valorar qué evidencias deben conservarse.

Primero se contiene el incidente. Después se analiza. Y posteriormente se recupera el entorno de forma segura.



14. Ransomware: cuando la información queda secuestrada

El ransomware bloquea o cifra información y posteriormente exige un pago para recuperarla.

La mejor defensa es haber preparado previamente el entorno: sistemas actualizados, accesos protegidos, personal formado, segmentación cuando proceda y, sobre todo, copias de seguridad recuperables y separadas del sistema afectado.

Durante la jornada se explicó el papel que pueden desempeñar especialistas en negociación y respuesta a incidentes dentro de determinadas pólizas de ciberriesgo.

Pero desde el punto de vista de la recomendación general de seguridad debe quedar claro que INCIBE aconseja no pagar el rescate.

Entre los motivos señala que pagar no garantiza recuperar la información, puede favorecer ataques posteriores y financia el negocio de los delincuentes.

Por tanto, aunque una póliza pueda contemplar diferentes gastos relacionados con un incidente, cualquier decisión ante una extorsión debe analizarse con especialistas, aseguradora y, cuando proceda, autoridades competentes.



15. Cuando todo falla: el papel del ciberseguro

Como explicó David Fernández Machi durante la jornada: «Hemos hablado de cómo te puede ayudar un seguro cuando todo falla.»

Un ciberseguro no sustituye las medidas de protección. Su función es ayudar a afrontar determinadas consecuencias una vez que el incidente se ha producido.

Dependiendo de la póliza contratada, las coberturas pueden incluir servicios de respuesta inmediata, análisis y contención del ataque, asistencia técnica y jurídica, recuperación de sistemas y datos, gastos de notificación, gestión de crisis, interrupción del negocio u otras pérdidas contempladas expresamente en el contrato.

Una de las ventajas destacadas durante el seminario es que permite a una pyme disponer, en el momento crítico, de profesionales especializados a los que probablemente no podría mantener permanentemente en plantilla.

Pero antes de contratar una póliza deben revisarse cuidadosamente los límites, exclusiones, franquicias, servicios incluidos, procedimiento de comunicación de incidentes y medidas mínimas de seguridad exigidas por la aseguradora.



16. La formación de las personas sigue siendo una de las principales defensas

La tecnología puede bloquear muchos ataques, pero una parte significativa del riesgo continúa dependiendo de las decisiones de las personas.

Josep García González destacó durante la jornada la importancia de la concienciación ante riesgos que cada vez aparecen con mayor frecuencia en situaciones reales del sector turístico.

Una política de ciberseguridad que nadie conoce tiene poca utilidad.

Todo el personal debería saber identificar al menos los principales indicadores de phishing; cómo actuar ante un cambio de cuenta bancaria; a quién comunicar un incidente; qué documentación puede almacenarse; qué canales están autorizados; qué hacer si pierde un dispositivo y qué comportamiento seguir cuando sospecha que ha cometido un error.

También debe existir una cultura que favorezca la comunicación inmediata.

Un empleado que ha pulsado un enlace fraudulento debe avisar cuanto antes.

Ocultar el error por miedo a las consecuencias puede hacer que un incidente inicialmente controlable se convierta en un problema grave.



17. El plan mínimo de ciberseguridad de una agencia de viajes

Una agencia no necesita convertirse en una empresa tecnológica para mejorar considerablemente su seguridad.

Necesita establecer procedimientos y cumplirlos.

Como mínimo, el plan debería contemplar:

1. Inventario actualizado de equipos, cuentas, aplicaciones y servicios.

2. Contraseñas únicas y gestor de contraseñas cuando proceda.

3. Doble factor activado en los servicios críticos.

4. Sistemas, programas y web actualizados.

5. Permisos limitados a las funciones de cada persona.

6. Copias de seguridad periódicas y al menos una separada del entorno principal.

7. Procedimiento específico para validar cambios de cuentas bancarias.

8. Normas claras sobre correo electrónico, dispositivos y mensajería.

9. Procedimiento para DNI, pasaportes y documentación médica.

10. Baja inmediata de accesos cuando una persona abandona la organización.

11. Protocolo para comunicar internamente cualquier incidente.

12. Lista de contactos técnicos, jurídicos, bancarios y aseguradores para emergencias.

13. Procedimiento de gestión de brechas de datos.

14. Formación periódica de todo el equipo.

15. Simulación ocasional de escenarios: phishing, caída de sistemas o fraude en pagos.
16. Revisión periódica del plan y de los riesgos.



18. Si ocurre mañana: la regla de oro

Cuando aparece una pantalla bloqueada, desaparecen archivos, un proveedor asegura que no ha recibido nuestro dinero o descubrimos que alguien ha accedido a una cuenta, el peor momento para diseñar un procedimiento es precisamente ese.

La agencia debería tener decidido de antemano:

01. A quién llamamos.

02. Quién toma las decisiones.

03. Cómo aislamos el problema.

04. Dónde están las copias. Cómo recuperamos la actividad.

05. Qué evidencias debemos conservar.

06. A quién debemos comunicar el incidente.

07. Y qué obligaciones legales debemos valorar.

La preparación no impide todos los ataques.

Pero sí puede marcar la diferencia entre un incidente controlado y una crisis que paralice la empresa durante días.



19. Recursos de ayuda

INCIBE mantiene el servicio 017 - Tu Ayuda en Ciberseguridad, gratuito y confidencial, dirigido también a empresas.

Actualmente presta atención los 365 días del año de 8:00 a 23:00 y dispone además de canales de WhatsApp, Telegram y formulario web.

La AEPD dispone de información específica y herramientas para gestionar y evaluar brechas de datos personales, entre ellas recursos para determinar cuándo procede la notificación a la autoridad o la comunicación a las personas afectadas.



MANUAL DE CIBERSEGURIDAD PARA AGENCIAS DE VIAJES

Una guía práctica elaborada a partir de los contenidos, recomendaciones y casos analizados durante la jornada de ciberseguridad organizada por AEVAV.

Prevención, protección de datos, fraude digital, respuesta ante incidentes y continuidad de la actividad.

Organiza:

AEVAV C.V.
ASOCIACIÓN EMPRESARIAL VALENCIANA DE AGENCIAS DE VIAJE

Con la colaboración de:

HISCOX
AON
LEY NET CONSULTORES