GUÍA VISUAL DE CIBERSEGURIDAD
para agencias de viajes

Las 10 cuestiones clave que debes tener en cuenta



Organiza:

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

Con la colaboración de:

HISCOX

AON

LEY NET CONSULTORES

Guía visual elaborada a partir de la jornada organizada por AEVAV

Octubre 2026

soloAgentes

1 Conoce tu infraestructura tecnológica

Antes de proteger, identifica todo lo que utilizas.

- Ordenadores y móviles
- Cuentas de correo y usuarios
- Programas y plataformas de reservas
- Datos y dónde se almacenan
- Quién tiene acceso
- Servicios contratados (nube, web, etc.)



2 Contraseñas y doble factor de autenticación

Tu primera línea de defensa.

- Usa contraseñas diferentes y robustas
- Emplea un gestor de contraseñas
- Activa el doble factor (2FA)
- No compartas contraseñas
- Especial atención al correo, banca y plataformas de reservas



3 Sistemas siempre actualizados

Evita vulnerabilidades conocidas.

- Mantén al día sistemas operativos
- Actualiza navegadores y aplicaciones
- Revisa programas de gestión
- Actualiza tu web y sus complementos
- No uses software obsoleto



4 El correo electrónico: identifica y evita el phishing

Desconfía, incluso si parece real.

- Revisa el remitente y los enlaces
- Desconfía de la urgencia
- No abras archivos no solicitados
- Verifica cambios de procedimientos
- Ante la duda, consulta por otro canal



5 Control de pagos y cambio de cuentas bancarias

Verifica siempre por un segundo canal.

- Desconfía de cambios de cuenta por email
- Confirma por teléfono con datos conocidos
- Comprueba la titularidad bancaria
- Extrema la revisión en nuevos proveedores
- En caso de fraude, contacta de inmediato con el banco



6 Copias de seguridad: tu mejor garantía

Para poder volver a trabajar.

- Realiza copias periódicas
- Almacénalas en un entorno separado
- Comprueba que se pueden recuperar
- Incluye toda la información crítica
- Combina copias locales y en la nube



7 DNI, pasaportes y documentación de clientes

Solo lo necesario y el tiempo imprescindible.

- Solicita únicamente los datos necesarios
- No conserves copias sin justificación
- Aplica el principio de minimización
- Protege el almacenamiento y el acceso
- Elimina la documentación cuando ya no sea necesaria



8 Datos médicos y otra información sensible

Requieren una protección especial.

- Trata solo la información necesaria
- Limita el acceso al personal autorizado
- Evita almacenarla innecesariamente
- Utiliza canales seguros
- Define un procedimiento claro de gestión y eliminación



9 Qué hacer ante un ciberataque

Actúa con rapidez y sigue un procedimiento.

- Aisla los equipos afectados
- Conserva las evidencias
- Bloquea accesos y cambia contraseñas
- Contacta con tus proveedores y aseguradora
- Valora la obligación de notificar
- Recupera la actividad de forma segura



10 Ciberseguro y recuperación de la actividad

Apoyo especializado cuando todo falla.

- Asistencia técnica y jurídica
- Gestión de crisis y recuperación de sistemas
- Cobertura de pérdidas y responsabilidad
- Revisa límites, exclusiones y franquicias
- Mantén tus medidas de seguridad al día
- Te ayuda a volver a la normalidad

