

## Política de la Extranet de Bookassist

Última actualización: 25 de mayo de 2018

La presente Política incluye:

- 1) Los términos y las condiciones relativos al uso del sistema de administración de Bookassist (en adelante, el «Sistema»)**
- 2) La información sobre protección de datos para los empleados / el personal autorizado que acceden al Sistema y/o al sistema de gestión de contenidos de Bookassist (en adelante, «CMS»)**
- 3) Notas explicativas sobre la Política de contraseñas para usar el Sistema**

Tenga en cuenta que al usar el sistema de administración de Bookassist (en adelante, el «Sistema») acepta los términos y condiciones aquí establecidos.

El Sistema ofrece acceso a datos personales basado en las obligaciones contractuales que se establecen en el Contrato de Bookassist con el proveedor de alojamiento y de conformidad con los Términos relativos a la seguridad i el tratamiento de datos de Bookassist (<https://bookassist.org/dp/es/>).

### **1) Términos y condiciones relativos al uso del sistema de administración de Bookassist (en adelante, el «Sistema»)**

#### **1. Requisitos de las PCI DSS (normas de seguridad de la información en la industria de medios de pago)**

- a) Aunque Bookassist hace todo lo posible por cumplir plenamente las condiciones estipuladas por las normas de seguridad de la información en la industria de medios de pago (PCI DSS) para el procesamiento de pagos en línea, el proveedor del alojamiento tiene la responsabilidad plena de usar correctamente los datos personales proporcionados en el Sistema de conformidad con la legislación pertinente en materia de protección de datos.
- b) El proveedor del alojamiento debe designar a un administrador para el Sistema, que será el responsable de controlar el acceso al Sistema por parte de otros empleados y/o personal autorizado (en adelante, los «Usuarios»).
- c) El proveedor del alojamiento reconoce su responsabilidad plena de asegurar el funcionamiento correcto de los requisitos de las PCI DSS implementadas por Bookassist con respecto a la administración de los Usuarios con acceso al Sistema, la protección de los nombres de usuario y contraseñas para el Sistema y, en particular, el control del acceso otorgado a los Usuarios a los datos de la tarjeta de crédito del titular de la misma. Concretamente, el proveedor del alojamiento:
  - o Garantiza que respetará los requisitos de seguridad de las PCI DSS.
  - o Reconoce su responsabilidad de asegurar los datos de los titulares de tarjetas.
  - o Reconoce que los datos de los titulares de tarjetas solo deben utilizarse para ayudar a la realización de una transacción, dar soporte a un programa de fidelidad o prestar un servicio de control contra el fraude, o bien para otros usos requeridos específicamente por ley.

- o Ofrecerá plena colaboración y acceso para llevar a cabo una revisión de seguridad exhaustiva tras una intrusión en el sistema de seguridad de un representante de la industria de medios de pago o de un tercero autorizado por dicha industria.
  - o Reconoce que las obligaciones de salvaguardar la confidencialidad de los datos de los titulares de tarjetas sobrevivirán a la terminación de otros acuerdos contractuales suscritos con Bookassist.
- d) La violación de las normas, procedimientos o directrices establecidos en virtud de esta Política se notificará a la Dirección del proveedor del alojamiento para que se tomen las acciones oportunas. Dichas acciones pueden incluir medidas disciplinarias, como el despido o la interrupción del servicio, y/o acciones legales.

## **2. Acceso en función de las necesidades de información**

El acceso a un nivel determinado del sistema solo debe otorgarse a los Usuarios que necesiten específicamente acceder a dicho nivel para realizar su trabajo.

## **3. Restricciones de acceso y de datos**

- a) Solo debe proporcionarse acceso si existe una autorización por parte del proveedor del alojamiento.
- b) Los datos de la tarjeta de crédito del cliente solo pueden visualizarse durante un mes como máximo a contar desde la fecha de salida del alojamiento que consta en la reserva. A partir de ese momento, los datos se eliminarán automáticamente del sistema de Bookassist y no podrán recuperarse.
- c) El resto de datos personales del cliente se anonimizarán transcurridos 12 meses desde la fecha de salida del alojamiento.

## **4. Datos de inicio de sesión personales**

Los datos de inicio de sesión deben ser únicos para cada usuario. Los usuarios no compartirán sus datos de inicio de sesión con ninguna otra persona.

## **5. Usuarios inactivos**

Deberán eliminarse inmediatamente los datos de inicio de sesión de los Usuarios que ya no los necesitan o que se han ido del hotel.

## **6. Usuarios nuevos**

Cuando se establecen datos de inicio de sesión para el Sistema, el usuario está obligado a leer, entender y aceptar las condiciones arriba mencionadas.

## **2) Información sobre protección de datos para los empleados / el personal autorizado que acceden al Sistema y/o al sistema de gestión de contenidos de Bookassist (en adelante, «CMS»)**

### **1. Información recopilada sobre los empleados / el personal autorizado (en adelante, los «Usuarios») que acceden al Sistema o al CMS y motivos por los cuales se recopila y se trata dicha información**

- a) Los usuarios que acceden al Sistema o al CMS deben proporcionar su nombre, su dirección de correo electrónico y su teléfono. Además, el Sistema y el CMS guardan información de registro de todos los accesos y actividades.
- b) Esta recopilación y tratamiento de datos es necesaria para la funcionalidad del Sistema y el CMS y para analizar problemas de modo que podamos gestionarlos.

## **2. Cómo se pueden usar los datos de los Usuarios y quién tiene acceso a dichos datos**

Los datos de los Usuarios se usarán para dar soporte al funcionamiento del Sistema y el CMS. El proveedor del alojamiento puede solicitar acceso a los datos del Usuario. Póngase en contacto con el proveedor del alojamiento en cuestión para obtener información sobre cómo utiliza estos datos de usuario. Tenga en cuenta que si el proveedor del alojamiento ha solicitado los datos de usuario, el proveedor puede conservar el acceso a esos datos durante un período de conservación diferente.

## **3. Derechos del Usuario**

El Usuario tiene derecho a solicitar el acceso, la rectificación y supresión de sus datos, así como derecho a la portabilidad de los datos y a presentar una reclamación ante la autoridad de control pertinente en virtud de los requisitos relevantes en materia de protección de datos.

## **4. Conservación**

Bookassist conservará todos los datos que se enumeran en el apartado 1 durante dos años a contar desde la fecha de caducidad del usuario.

## **5. Contacto**

Para obtener información adicional o ejercer sus derechos, escriba un correo electrónico a la persona de contacto de Protección de datos de Bookassist a la dirección [dpo@bookassist.com](mailto:dpo@bookassist.com).

## **3) Notas explicativas sobre la Política de contraseñas para usar el Sistema**

Las normas de la PCI establecen que las contraseñas que utiliza en el Sistema deben cumplir un conjunto de normas específicas. El procedimiento de inicio de sesión en el Sistema garantiza el cumplimiento de las normas de la PCI. La comprobación de inicio de sesión de Bookassist validará el nombre de usuario y la contraseña, y en caso de errores mostrará mensajes claros en la pantalla para explicar cuál es el problema y cómo subsanarlo.

### **1. Contraseñas seguras**

Seleccione contraseñas seguras con estas características:

- Utilice mayúsculas y minúsculas, y números o caracteres de puntuación;
- no utilice información personal o palabras de uso común o que se puedan encontrar en un diccionario;
- no comparta la contraseña con nadie;
- no anote la contraseña ni la guarde en línea.

### **2. Caducidad de la contraseña**

Cada 90 días, el Sistema le pedirá que cambie su contraseña. Se mostrarán instrucciones claras para realizar este proceso.

### **3. Formato de la contraseña**

La contraseña debe tener como mínimo 7 caracteres, con al menos 1 número y 1 carácter del alfabeto. Si cambia la contraseña y no cumple estos requisitos, aparecerá un mensaje en la pantalla para indicarle cómo crear una contraseña válida.

### **4. Historial de contraseñas**

Al cambiar la contraseña, el Sistema comprueba que no coincida con ninguna de las 4 últimas contraseñas que ha usado.

### **5. Intentos de inicio de sesión**

Si está iniciando sesión e introduce una contraseña incorrecta, tiene un total de 6 intentos antes de que se le bloquee el acceso. Si esto ocurre, solicítele a su administrador que restablezca la contraseña y espere 30 minutos para volver a iniciar sesión.

### **6. Tiempo de bloqueo**

Si se ha bloqueado su acceso al Sistema porque ha introducido una contraseña incorrecta 6 veces, debe esperar 30 minutos para poder iniciar sesión de nuevo, incluso en caso de que el administrador haya restablecido su contraseña.

### **7. Tiempo de espera de la sesión**

La PCI requiere que limitemos una sesión iniciada a 15 minutos de inactividad. Si su ordenador ha estado inactivo durante más de 15 minutos, deberá volver a iniciar sesión en el Sistema.

### **8. Caducidad del usuario**

Si no ha iniciado sesión en el sistema durante 90 días, su usuario caduca y debe pedirle al administrador que lo restablezca.

### **9. Usuario nuevo o restablecimiento de la contraseña**

En el caso de un usuario nuevo al que se enviado una contraseña temporal, o un usuario que ha solicitado el restablecimiento de su contraseña y al que se enviado una contraseña temporal, el usuario debe iniciar sesión con la contraseña temporal en un plazo de 24 horas. Transcurrido este plazo, la contraseña habrá caducado y el administrador deberá restablecerla.