

Implementación de las DSS de la PCI por Bookassist Versión 2.0 del documento

Acerca de las DSS de la PCI

Las normas de seguridad para realizar pagos en línea se denominan Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (DSS de la PCI, de sus siglas en inglés) y representan los requisitos de buenas prácticas de Visa y Mastercard para el procesamiento de tarjetas de crédito en línea. Dichas normas le protegen a usted y a Bookassist de las consecuencias de un acceso fraudulento a las tarjetas de crédito del cliente.

Bookassist facilita a los hoteles toda la información que necesitan para implementar estas normas de seguridad. No obstante, es responsabilidad de los hoteles que utilizan el sistema de administración de Bookassist garantizar que usan el sistema de un modo conforme a los requisitos de la PCI. Con ese fin, los hoteles deben nombrar un administrador para el sistema de administración de Bookassist, que será el responsable de controlar el acceso de otros usuarios del hotel.

Tenga en cuenta que al utilizar el sistema de administración de Bookassist acepta los términos y condiciones que se describen en este documento.

Términos y condiciones

1. Requisitos de protección de datos y de la Industria de Tarjetas de Pago (PCI)

Bookassist se compromete a cumplir debidamente los requisitos de la Ley de Protección de Datos de 1988 (en esta cláusula, «la Ley»), entre los que se incluyen: a) los principios de protección de datos estipulados en la Ley; b) las peticiones de las personas a las que se refieren los datos para acceder a dichos datos; y c) los requisitos relacionados con el registro de usuarios. La divulgación o transferencia de datos por parte de Bookassist a personas que tengan el consentimiento explícito de terceros para hacerlo debe cumplir la legislación de protección de datos aplicable. En la presente cláusula, «datos» hace referencia a toda la información que terceras personas han facilitado o facilitarán a Bookassist o al proveedor de alojamiento, incluidos los datos de solicitudes, reservas y transacciones respecto de la información de pago con tarjeta de crédito u otros datos.

Bookassist hace todo lo posible por cumplir plenamente las condiciones estipuladas en las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (DSS de las PCI) para el procesamiento de pagos en línea.

El proveedor de alojamiento asumirá toda la responsabilidad en cuanto a la correcta aplicación de los requisitos de las DSS de la PCI implementados por Bookassist con respecto a los siguientes aspectos: la gestión de usuarios locales con acceso al sistema de administración de hoteles de Bookassist, la protección de nombres de usuario y contraseñas para el sistema y, en particular, el control de los permisos concedidos a los usuarios para acceder a los datos de las tarjetas de crédito de los clientes. Concretamente, el proveedor de alojamiento garantiza que:

- se adhiere a los requisitos de las DSS de la PCI;
- acepta su responsabilidad de garantizar la seguridad de los datos del titular de la tarjeta;
- acepta que los datos del titular de la tarjeta solo deben usarse en los siguientes casos: ayudar a concluir una transacción, respaldar un programa de fidelidad, ofrecer un servicio de control de fraude u otros usos específicamente exigidos por ley;
- cooperará y facilitará acceso total para llevar a cabo una revisión de seguridad completa tras una intrusión de seguridad a un representante de la industria de tarjetas de pago o a un tercero autorizado por la industria de tarjetas de pago;
- acepta que dichas obligaciones de salvaguardar la confidencialidad de los datos del titular de la tarjeta deben continuar una vez terminado cualquier acuerdo contractual con Bookassist.

Todo incumplimiento de las normas, procedimientos o directrices establecidos de acuerdo con esta política será puesto en conocimiento de la dirección del proveedor de alojamiento para que tome las medidas pertinentes. Esto podría dar lugar a la aplicación de medidas disciplinarias como el despido o la cesación del servicio y/o el ejercicio de acciones legales.

2. Información detallada

Acceso en función de la necesidad de conocer de los usuarios

Solo deben obtener acceso a un nivel determinado en el sistema los usuarios que necesiten específicamente obtener acceso a ese nivel para desempeñar su trabajo.

Restricciones de acceso y datos

El acceso debe ser autorizado por el cliente/director del hotel o por el director de reservas.

Los datos del titular de la tarjeta solo se podrán consultar hasta un mes después de la fecha de salida del cliente. Después de dicha fecha, la información se eliminará automáticamente del sistema de Bookassist y no se podrá recuperar.

Datos de inicio de sesión individuales

Los datos de inicio de sesión deben ser exclusivos de cada usuario. Los usuarios no deben compartir sus datos de inicio de sesión con terceros.

Usuarios inactivos

Deben eliminarse inmediatamente los datos de inicio de sesión del personal que ya no los necesite o que ya no trabaje en el hotel.

Usuarios nuevos

Al configurar los datos de inicio de sesión para el sistema de administración de Bookassist, el usuario debe leer, entender y aceptar las condiciones mencionadas anteriormente.

Notas explicativas sobre la política de contraseñas

Las normas de la PCI exigen que las contraseñas utilizadas por usted en el sistema de administración de Bookassist cumplan un conjunto de normas. El procedimiento de inicio de sesión en el sistema garantiza que se cumplen dichas normas. La comprobación de los datos de inicio de sesión de Bookassist validará el nombre de usuario y la contraseña y, en caso de que se produzca un error, mostrará un mensaje claro en la pantalla para explicar cuál es el problema y cómo corregirlo.

Contraseñas seguras

Elija contraseñas seguras que cumplan los siguientes requisitos:

- utilice mayúsculas y minúsculas, números y signos de puntuación;
- no utilice información personal ni palabras de uso común o que figuren en un diccionario;
- no comparta la contraseña con nadie;
- no escriba la contraseña en un papel ni la guarde en ningún lugar en línea.

Duración de la contraseña

Cada 90 días, el sistema le pedirá que cambie la contraseña. Las instrucciones le indicarán cómo hacerlo.

Formato de la contraseña

La contraseña debe tener una longitud mínima de siete caracteres, entre los cuales debe haber, por lo menos, un número y un carácter alfabético. Si cambia la contraseña y esta no cumple los requisitos, aparecerá un mensaje en la pantalla que le indicará qué hacer para introducir una contraseña válida.

Historial de contraseñas

Cuando cambia su contraseña, el sistema comprueba que no coincida con ninguna de las últimas cuatro que ha utilizado.

Intentos de inicio de sesión

Si introduce una contraseña incorrecta al iniciar sesión, tiene seis intentos en total antes de que se le bloquee el acceso. En caso de bloqueo, diríjase a su administrador para restablecer la contraseña y espere 30 minutos para volver a iniciar sesión.

Tiempo de bloqueo

Si se le ha bloqueado el acceso al sistema porque ha introducido una contraseña incorrecta seis veces, debe esperar 30 minutos antes de volver a iniciar sesión, aunque el administrador haya restablecido su contraseña.

Finalización de la sesión

La PCI nos exige cerrar la sesión después de 15 minutos sin actividad. Si su ordenador ha estado inactivo durante más de 15 minutos, deberá volver a iniciar sesión en el sistema.

Usuario caducado

Si no ha iniciado sesión en el sistema en los últimos 90 días, su nombre de usuario caduca y debe pedir a su administrador que lo restablezca.

Nuevo usuario o restablecimiento de la contraseña

Un usuario nuevo que ha recibido una contraseña temporal o un usuario que ha solicitado restablecer la contraseña y ha recibido una nueva contraseña temporal debe iniciar sesión con la contraseña temporal en un plazo de 24 horas. Después de ese plazo, la contraseña temporal caduca y el administrador debe restablecerla.