

MATERIALES DE VENDOCERTA

Seguridad y RGPD

La protección de datos en VendoCerta está repartida por todo el producto: cómo se escribe el historial, quién puede ver qué documento, cómo se cifra la cuenta bancaria, y qué no puede hacer un rol de forma deliberada. Esta página lo reúne todo en un solo lugar.

5

roles con funciones
separadas

5

reglas que ningún rol
elude

AES-256

cifrado de datos
sensibles

Seis preguntas que surgen primero.

¿Pueden los datos quedarse con nosotros?

Sí. VendoCerta se instala en una infraestructura que ustedes controlan.

¿Cómo se protegen los datos sensibles?

AES-256-GCM en reposo; revelarlos exige volver a introducir la contraseña y un motivo que queda registrado en el historial.

¿Quién tiene acceso a qué?

Roles con una separación de funciones real. Nadie cambia su propio rol.

¿Hay un segundo factor de inicio de sesión?

Sí, obligatorio para los roles con acceso a datos del negocio.

¿Puede una sola persona cambiar la cuenta bancaria de un proveedor?

No. Cuatro etapas, roles separados, al menos dos personas.

¿Se puede corregir el historial de auditoría?

No. No hay función de edición ni de eliminación en la interfaz, en ningún rol, ni siquiera para el propietario.

Una entrada no se puede modificar ni eliminar. Ni siquiera el propietario.

Cada acción registrada se convierte en una entrada: inicio de sesión, cambio de estado de un proveedor, decisión sobre un documento, invitación enviada, archivo descargado. VendoCerta no tiene en ningún sitio una función para editar o eliminar una entrada, y nunca sobrescribe un evento existente.

Antes y después, en cada cambio de datos

Cada entrada lleva: quién, qué, cuándo — y en un cambio, también cómo eran los valores en ambos lados.

Los rechazos también se registran

Si alguien intenta abrir algo para lo que no tiene permiso, ese intento es una entrada. Los intentos repetidos quedan así visibles, no silenciosos.

Una vista filtrada es un enlace

Los filtros se reflejan en la dirección de la página, así que un fragmento concreto del historial puede compartirse con un colega — o un auditor — como una dirección.

Retención propia — y lo decimos abiertamente

El número de días al pie de la pantalla del historial de auditoría no es el mismo campo que el de la pantalla de ajustes. La retención del historial de auditoría es un ajuste independiente, que actualmente no se puede cambiar desde la interfaz, y cambiar el otro campo no lo afecta.

La única operación cuya facilitación el producto se niega a dar.

Cambiar la cuenta bancaria de un proveedor consta de cuatro etapas y una regla sobre quién puede completarlas. Todo lo demás en VendoCerta está diseñado para eliminar fricción; esto está diseñado para conservarla.

Cifrado desde el momento del guardado

El número de cuenta nunca se guarda en texto plano en la base de datos — AES-256-GCM en reposo, desde el momento del guardado.

Revelarlo cuesta tres cosas

El permiso para datos sensibles, volver a introducir la contraseña pese a estar conectado, y dar un motivo que queda en el historial. El motivo se guarda; el número nunca. El número desaparece de la pantalla a los 45 segundos.

Los duplicados se muestran, no se ocultan

Si el mismo número de cuenta ya figura en otro proveedor, la advertencia debe descartarse conscientemente antes de que la aprobación siquiera sea posible.

Cinco roles, y el sorprendente es intencionado.

El administrador de sistemas mantiene la instalación sana — configuración, diagnósticos, copias de seguridad — y no tiene ningún acceso a proveedores, documentos, casos ni cuentas bancarias. Justo lo contrario del administrador de negocio, que dirige el lado de proveedores y no puede restaurar una copia de seguridad.

CAPACIDAD	PROPIETARIO	ADMINISTRADOR DE NEGOCIO	ADMINISTRADOR DE SISTEMAS	REVISOR	OBSERVADOR
Ve proveedores y documentos	✓	✓	—	✓	✓
Añade y edita proveedores	✓	✓	—	—	—
Revisa documentos y decide la aprobación	✓	✓	—	✓	—
Ve documentos sensibles (datos de pago)	✓	✓	—	—	—
Gestiona usuarios y roles	✓	✓	✓	—	—
Restaura una copia de seguridad	✓	—	—	—	—

Reglas que ningún rol puede eludir

- Nadie — incluido el propietario — puede cambiar su propio rol.
- Un administrador no puede crear ni degradar una cuenta con el rol de propietario.
- La última cuenta de propietario no se puede degradar ni desactivar, así que la empresa nunca se queda sin nadie con permisos completos.
- La autenticación de dos factores es obligatoria e ineludible para el propietario, el administrador de negocio, el administrador de sistemas y el revisor. El observador puede activarla, pero no está obligado.
- Un inicio de sesión fallido nunca revela si el correo o la contraseña eran incorrectos, así que la pantalla no puede usarse para comprobar si existe una cuenta.

Qué se guarda, quién puede acceder a ello y durante cuánto tiempo.

Los documentos sensibles requieren un permiso aparte

Los documentos ordinarios de un proveedor los ve cualquiera con acceso a su ficha. Los documentos marcados como sensibles — sobre todo relacionados con pagos — requieren un permiso adicional, que en la práctica solo tienen el propietario y el administrador. Un intento sin él termina en rechazo, y el rechazo queda registrado.

Los archivos nunca tienen una dirección fija

La descarga pasa por un enlace firmado digitalmente, válido durante unos minutos y vinculado a su empresa. Abrirlo desde otro contexto no sirve de nada. Cada descarga de un archivo sensible se audita por separado.

Retención: siete años por defecto

El ajuste de documentos y retención está por defecto en 2555 días, conforme a los requisitos habituales de auditoría de compras, y puede cambiarse en cualquier momento. Con honestidad: hoy registra su política y guiará las futuras limpiezas — nada se elimina automáticamente solo porque venza un plazo.

Las invitaciones caducan, y reenviar las invalida

El enlace de invitación es un token aleatorio con vida limitada, una semana por defecto — deliberadamente no de un solo uso, para que el proveedor pueda volver a un formulario sin terminar con el mismo enlace. Enviar una nueva invitación invalida de inmediato la anterior, aunque ya se haya abierto — hoy es la única forma de cortar un enlace; no existe un botón de revocación aparte.

Datos bancarios cifrados en reposo

AES-256-GCM desde el momento del guardado. El motivo indicado para revelar el número va al historial de auditoría; el número en sí, nunca.

Informe de soporte sin datos

La pestaña de diagnóstico del centro del sistema genera un informe para el soporte técnico con versiones, contadores y líneas de registro enmascaradas — nunca el contenido de documentos, datos bancarios ni datos personales de proveedores.

Las preguntas que un auditor hace primero.

¿Es VendoCerta un servicio en la nube al que confiamos los datos?

No. Se instala en una máquina que ustedes controlan. PostgreSQL, el almacenamiento de archivos y la vista previa de correo funcionan como binarios portables dentro de la carpeta del proyecto — nada se instala a nivel de Windows, sin permisos de administrador, Docker es opcional. Se necesita Internet en el primer arranque para descargar estos servicios; después, la instalación es suya.

¿Recibimos documentación técnica más allá de esta página?

Sí. La instalación incluye un modelo de seguridad y un modelo de amenazas como documentos en el repositorio — las mismas fuentes de las que salió esta página. Pídanse los a quien mantenga su instalación, o a nosotros mediante el formulario de demostración, indicando que es para una revisión de seguridad.

¿A qué tiene acceso el asistente de IA?

Solo a lo que la persona que pregunta ya puede ver, y nunca ejecuta una acción sin su confirmación explícita — los permisos se comprueban de nuevo en el momento del clic, contra la persona que hace clic. No puede aprobar, rechazar ni suspender a un proveedor, no puede cambiar un rol y no puede eliminar nada.

¿El restablecimiento de contraseña permite saltarse la autenticación de dos factores?

No. Para los roles en los que el segundo factor es obligatorio, lo es en cualquier vía hacia la cuenta, también tras un restablecimiento.

¿A dónde van los correos durante el piloto?

A un buzón de vista previa local en la propia instalación, no a destinatarios reales — para que el piloto no pueda escribir por accidente a un proveedor. La pestaña de instalación del centro del sistema indica qué buzón usa realmente una instalación concreta.