

MATERIALI VENDOCERTA

Sicurezza e RODO

La protezione dei dati in VendoCerta è distribuita in tutto il prodotto: come viene scritta la cronologia, chi può vedere quale documento, come viene cifrato il conto bancario, e cosa un ruolo non può fare deliberatamente. Questa pagina riunisce tutto in un unico posto.

5

ruoli con poteri separati

5

regole che nessun ruolo aggira

AES-256

cifatura dei dati sensibili

Sei domande che arrivano per prime.

I dati possono restare da noi?

Sì. VendoCerta si installa su un'infrastruttura che controllate voi.

Come vengono protetti i dati sensibili?

AES-256-GCM a riposo; la rivelazione richiede una nuova password e un motivo salvato nella cronologia.

Chi ha accesso a cosa?

Ruoli con una reale separazione dei compiti. Nessuno cambia il proprio ruolo.

C'è un secondo fattore di accesso?

Sì, obbligatorio per i ruoli con accesso ai dati aziendali.

Una sola persona può cambiare il conto bancario di un fornitore?

No. Quattro fasi, ruoli separati, almeno due persone.

La cronologia di audit può essere corretta?

No. Nessuna funzione di modifica o eliminazione nell'interfaccia, in nessun ruolo, nemmeno per il proprietario.

Una voce non può essere modificata né eliminata. Nemmeno dal proprietario.

Ogni azione salvata diventa una voce: accesso, cambio di stato di un fornitore, decisione su un documento, invito inviato, file scaricato. VendoCerta non ha da nessuna parte una funzione per modificare o eliminare una voce e non sovrascrive mai un evento esistente.

Prima e dopo, a ogni modifica dei dati

Ogni voce riporta: chi, cosa, quando — e in caso di modifica, anche come apparivano i valori su entrambi i lati.

Anche i rifiuti vengono registrati

Se qualcuno tenta di aprire qualcosa a cui non ha diritto, quel tentativo diventa una voce. I tentativi ripetuti sono quindi visibili, non silenziosi.

Una vista filtrata è un link

I filtri si riflettono nell'indirizzo della pagina, così un frammento preciso della cronologia può essere condiviso — con un collega o un revisore — come indirizzo.

Conservazione propria — e lo diciamo apertamente

Il numero di giorni in fondo alla schermata della cronologia di audit non è lo stesso campo di quello nella schermata delle impostazioni. La conservazione della cronologia di audit è un'impostazione separata, attualmente non modificabile dall'interfaccia, e modificare l'altro campo non la influenza.

L'unica operazione che il prodotto rifiuta di facilitare.

Cambiare il conto bancario di un fornitore prevede quattro fasi e una regola su chi può completarle. Tutto il resto in VendoCerta è progettato per rimuovere attrito; questo è progettato per mantenerlo.

Cifrato dal momento del salvataggio

Il numero di conto non risiede mai in chiaro nel database — AES-256-GCM a riposo, dal momento del salvataggio.

La rivelazione costa tre cose

Il diritto sui dati sensibili, una nuova immissione della password nonostante l'accesso attivo, e un motivo che finisce nella cronologia. Il motivo viene salvato; il numero mai. Il numero scompare dallo schermo dopo 45 secondi.

I duplicati vengono mostrati, non nascosti

Se lo stesso numero di conto è già presente presso un altro fornitore, l'avviso deve essere scartato consapevolmente prima che l'approvazione diventi possibile.

Cinque ruoli, e quello sorprendente è voluto.

L'amministratore di sistema mantiene sana l'installazione — configurazione, diagnostica, backup — e non ha alcun accesso a fornitori, documenti, pratiche o conti bancari. Esattamente l'opposto dell'amministratore aziendale, che gestisce il lato fornitori e non può ripristinare un backup.

FUNZIONALITÀ	PROPRIETARIO	AMMINISTRATORE AZIENDALE	AMMINISTRATORE DI SISTEMA	REVISORE	VISUALIZZATORE
Vede fornitori e documenti	✓	✓	—	✓	✓
Aggiunge e modifica fornitori	✓	✓	—	—	—
Verifica i documenti e decide sull'approvazione	✓	✓	—	✓	—
Vede documenti sensibili (dati di pagamento)	✓	✓	—	—	—
Gestisce utenti e ruoli	✓	✓	✓	—	—
Ripristina un backup	✓	—	—	—	—

Regole che nessun ruolo può aggirare

- Nessuno — nemmeno il proprietario — può cambiare il proprio ruolo.
- Un amministratore non può creare né retrocedere un account con il ruolo di proprietario.
- L'ultimo account proprietario non può essere retrocesso né disattivato, così l'azienda non resta mai senza nessuno con pieni poteri.
- L'autenticazione a due fattori è obbligatoria e non aggirabile per proprietario, amministratore aziendale, amministratore di sistema e revisore. L'osservatore può attivarla, ma non è obbligato.
- Un accesso fallito non rivela mai se era sbagliato l'indirizzo o la password, quindi la schermata non può essere usata per verificare se un account esiste.

Cosa viene conservato, chi può accedervi e per quanto tempo.

I documenti sensibili richiedono un diritto separato

I documenti ordinari del fornitore sono visibili a chiunque abbia accesso alla sua scheda. I documenti contrassegnati come sensibili — per lo più legati ai pagamenti — richiedono un diritto aggiuntivo, in pratica riservato solo a proprietario e amministratore. Un tentativo senza questo diritto termina con un rifiuto, e il rifiuto viene registrato.

I file non hanno mai un indirizzo fisso

Il download avviene tramite un link firmato digitalmente, valido per pochi minuti e legato alla vostra azienda. Aprirlo da un altro contesto non serve a nulla. Ogni download di un file sensibile viene registrato separatamente.

Conservazione: sette anni di default

L'impostazione di documenti e conservazione è di default a 2555 giorni, conforme ai tipici requisiti di audit degli acquisti, e può essere modificata in qualsiasi momento. In tutta onestà: oggi registra la vostra politica e guiderà le future pulizie — nulla viene eliminato automaticamente solo perché un termine è scaduto.

Gli inviti scadono, e un nuovo invio li invalida

Il link di invito è un token casuale con durata limitata, una settimana di default — volutamente non monouso, così il fornitore può tornare a un modulo incompleto con lo stesso link. L'invio di un nuovo invito invalida immediatamente il precedente, anche se è già stato aperto — oggi è l'unico modo per tagliare un link; non esiste un pulsante di revoca separato.

Dati bancari cifrati a riposo

AES-256-GCM dal momento del salvataggio. Il motivo indicato per rivelare il numero finisce nella cronologia di audit; il numero stesso mai.

Report di supporto senza dati

La scheda diagnostica nel centro di sistema genera un report per il supporto tecnico con versioni, contatori e righe di log mascherate — mai il contenuto dei documenti, i dati bancari o i dati personali dei fornitori.

Le domande che un revisore fa per prime.

VendoCerta è un servizio cloud a cui affidiamo i dati?

No. L'installazione avviene su una macchina che controllate voi. PostgreSQL, l'archiviazione file e l'anteprima e-mail funzionano come binari portabili all'interno della cartella del progetto — nulla viene installato a livello di Windows, senza diritti di amministratore, Docker è opzionale. Internet serve al primo avvio per scaricare questi servizi; dopodiché l'installazione è vostra.

Riceviamo documentazione tecnica oltre questa pagina?

Sì. L'installazione include un modello di sicurezza e un modello delle minacce come documenti nel repository — le stesse fonti da cui è nata questa pagina. Chiedeteli a chi gestisce la vostra installazione, o a noi tramite il modulo demo, specificando che servono per una revisione di sicurezza.

A cosa ha accesso l'assistente IA?

Solo a ciò che la persona che chiede può già vedere, e non esegue mai un'azione senza la sua conferma esplicita — i diritti vengono riverificati al momento del clic, sulla persona che clicca. Non può approvare, rifiutare o sospendere un fornitore, non può cambiare un ruolo e non può eliminare nulla.

Il reset della password aggira l'autenticazione a due fattori?

No. Per i ruoli in cui il secondo fattore è obbligatorio, lo è su ogni percorso verso l'account, anche dopo un reset.

Dove vanno le e-mail durante il pilota?

In una casella di anteprima locale sull'installazione stessa, non a destinatari reali — così il pilota non può scrivere per errore a un fornitore. La scheda installazione nel centro di sistema indica quale casella usa realmente una determinata installazione.