BMS

BUSINESS MANAGEMENT SYSTEM

DOCUMENTO CONFIDENCIAL

Politica de Seguridad de la Informacion

Controles tecnicos, organizacionales y de operacion implementados en la plataforma BMS para proteger los datos de las empresas clientes.

PLATAFORMA
BMS · Business Management System

FECHA DE EMISION
2026-05-08

VERSION
1.0

1. Proposito

Este documento describe los controles tecnicos, organizacionales y de operacion implementados en la plataforma BMS para proteger la confidencialidad, integridad y disponibilidad de los datos de las empresas clientes. Sirve como anexo al contrato de servicio.

2. Alcance

- La aplicacion web BMS (frontend, APIs, base de datos, almacenamiento de respaldos).
- Datos cargados por las empresas clientes en la plataforma.
- Personal autorizado de BMS con acceso administrativo.

3. Arquitectura multi-tenant

BMS opera bajo un modelo SaaS con aislamiento logico de datos por empresa:

- Cada empresa cliente recibe un identificador unico (empresaId) presente en mas de 100 tablas con indices y llaves foraneas.
- Una capa de software inyecta automaticamente el filtro WHERE empresaId en CADA consulta del sistema.
- Un usuario de la empresa A no puede, bajo ningun flujo del sistema, acceder a datos de la empresa B.
- Pruebas de regresion validan el aislamiento antes de cada despliegue.

> Demostracion: la plataforma cuenta con una empresa de prueba (DEMO) que valida en cada despliegue que los conteos de registros coinciden solo con datos cargados por DEMO.

4. Autenticacion y control de acceso

4.1 Politica de contrasenas

- Minimo 10 caracteres.
- Al menos una mayuscula, una minuscula, un numero y un simbolo.

- No estar en blacklist de contrasenas comunes.

4.2 Bloqueo por intentos fallidos

Tras 5 intentos consecutivos fallidos, la cuenta se bloquea automaticamente por 15 minutos. Solo un administrador puede desbloquearla antes.

4.3 Doble factor (MFA)

- TOTP compatible con Google Authenticator, Microsoft Authenticator, Authy, 1Password.
- 8 codigos de respaldo de un solo uso, hasheados con bcrypt.
- Administradores pueden forzar MFA o resetearlo si el usuario pierde acceso.

4.4 Sesiones

- JWT firmados con clave secreta rotable.
- Cookie con flags Secure, HttpOnly y SameSite=Lax.
- El token incluye empresaId para el filtrado multi-tenant.

4.5 Roles

Rol	Alcance
superadmin	Equipo BMS · gestiona empresas clientes
admin	Administrador interno de la empresa cliente
operator	Usuario operativo, scopeado a un area
vendedor	Portal restringido para vendedores

5. Bitacora de auditoria

La plataforma registra eventos criticos en una tabla AuditLog indexada por empresa, usuario, accion y fecha. Cada entrada captura: fecha exacta, usuario actor, accion, entidad afectada, estado anterior y nuevo, IP, user agent, exito o motivo de fallo.

Eventos auditados

- Autenticacion: login exitoso/fallido, bloqueo, cambio de password, MFA on/off.
- Gestion de usuarios: alta, edicion, activacion, desactivacion, eliminacion, desbloqueo, reset MFA.
- Gestion de empresas (BMS interno): creacion, edicion, suspension, reactivacion, eliminacion.
- Respaldos: generacion de snapshots, descargas.

> Privacidad: contrasenas y secretos MFA se redactan automaticamente como [REDACTED] antes de persistirse en la bitacora.

Visibilidad

- Cada empresa cliente ve unicamente la bitacora de su empresa.
- BMS internamente ve la bitacora consolidada (rol superadmin).

6. Cifrado

Capa	Cifrado
Cliente ” Servidor	TLS 1.2+ (HTTPS forzado)
Datos en reposo	AES-256 gestionado por Neon Postgres
Contrasenas	bcrypt con factor de costo 10
Tokens MFA TOTP	Almacenados cifrados; nunca se devuelven al cliente tras setup
Codigos respaldo MFA	Hash bcrypt, nunca en texto plano
Backups	Cifrados en reposo en Neon (PITR)

7. Respaldos y recuperacion ante desastres

BMS opera con tres capas independientes de respaldo:

- **Capa 1 — Neon PITR:** respaldos continuos con recuperacion punto-en-tiempo. Retencion 7 a 60 dias segun plan.
- **Capa 2 — Snapshot manual:** cualquier admin puede generar bajo demanda un export JSON completo de su empresa.
- **Capa 3 — Backup local interno:** equipo BMS conserva snapshots periodicos en almacenamiento independiente.

Objetivos de servicio

Metrica	Compromiso
RTO	d 4horas para incidentes mayores
RPO	d 24horas de perdida maxima de datos

Cada trimestre, BMS ejecuta una prueba de restauracion usando un snapshot real en una rama aislada de la base de datos. El resultado se documenta en el runbook interno de DR.

8. Disponibilidad

- Hospedaje frontend y APIs: Vercel (red global de edge).
- Hospedaje base de datos: Neon Postgres (multi-AZ).
- Despliegues: rolling deployments con health checks; rollback automatico.
- Monitoreo: bitacora de errores y disponibilidad continua.

> SLA objetivo: 99.5% mensual (H 3.6 horas maximas de no-disponibilidad por mes). Ventanas de mantenimiento programado se anuncian con al menos 48 horas de anticipacion.

9. Privacidad y manejo de datos

9.1 Propiedad de los datos

Los datos cargados por una empresa cliente son propiedad exclusiva del cliente. BMS actua como encargado del tratamiento.

9.2 Uso de los datos por BMS

BMS no comparte, vende ni utiliza los datos de las empresas clientes para fines distintos a la operacion del servicio. No se usan datos de clientes para entrenamiento de modelos de IA.

9.3 Personal con acceso

Solo personal autorizado de BMS, con rol superadmin y MFA obligatoria, puede acceder al panel administrativo cross-empresa. Cada acceso queda registrado en bitacora.

9.4 Portabilidad

A solicitud del cliente, BMS entrega un snapshot completo en formato JSON abierto. El cliente puede importar o procesar estos datos en cualquier sistema.

9.5 Eliminacion de datos

- Suspension inmediata al cancelar (datos siguen disponibles para descarga).
- Periodo de gracia de 30 dias.

- Eliminacion permanente de todos los registros tras el periodo de gracia.
- Registro en bitacora del proceso de eliminacion.

10. Gestion de incidentes

- **Deteccion:** monitoreo continuo + alertas automaticas.
- **Contencion:** suspension inmediata de servicios afectados si aplica.
- **Notificacion:** empresas clientes afectadas notificadas en plazo maximo de 72 horas.
- **Post-mortem:** documentado y compartido con clientes afectados.

11. Cumplimiento

BMS sigue las buenas practicas de seguridad SaaS segun ISO 27001 y SOC 2 Type II.

Una certificacion formal (ISO 27001 / SOC 2) esta en el roadmap del producto y se proveera a los clientes una vez completada.

12. Responsabilidades del cliente

El cliente se compromete a:

- Mantener confidenciales las credenciales de sus usuarios.
- Activar MFA en al menos los usuarios con rol de administrador.
- Revocar accesos de empleados que dejen la organizacion.
- Notificar a BMS cualquier sospecha de compromiso de cuenta.
- Almacenar de forma segura los snapshots descargados.

13. Contacto

Asunto	Contacto
Soporte general	contacto@bms.services
Reportes de seguridad	contacto@bms.services
Solicitud de auditoria	contacto@bms.services

14. Cambios al documento

Version	Fecha	Cambio
1.0	2026-05-08	Version inicial publicada