redsmart RH



SEGURIDAD Y PROTECCIÓN DE DATOS

Aislamiento de datos entre tenants y medidas de seguridad

Cómo RedSmart RH garantiza que la información de cada organización permanece separada, protegida y bajo su control.

Documento técnico · Julio 2026 · v1.0

RedSmart RH — Plataforma de cumplimiento laboral · por Go4IT

SECCIÓN 00

Resumen ejecutivo

RedSmart RH es una plataforma **multi-tenant** (multi-empresa) de marca blanca: varias organizaciones —llamadas tenants— operan sobre la misma infraestructura, pero sus datos permanecen estrictamente separados. Este documento describe, con evidencia verificada en producción, cómo garantizamos ese aislamiento y qué medidas adicionales protegen la información — en particular los datos personales **sensibles** de los colaboradores (salud, biométricos, nómina), regulados en México por la LFPDPPP.

IDEA CENTRAL

Ninguna petición puede pedir datos de otro tenant. La identidad de la organización nunca viaja como un parámetro que el cliente pueda modificar: se deriva del credencial autenticado y se aplica en dos capas independientes — la aplicación y el motor de base de datos.

SECCIÓN 01

Modelo multi-tenant: el concepto de «origen»

Cada registro de la plataforma lleva una etiqueta de tenant, el **origen**, que identifica a la organización dueña del dato. Al autenticarse, el sistema determina el **origen** del usuario a partir de su credencial — **no** de lo que envíe el cliente — y lo propaga a toda la petición. A partir de ahí, toda lectura y escritura queda acotada a ese origen. Es una separación **por diseño**, no una bandera que se pueda pedir de otra forma.

SECCIÓN 02

Aislamiento en dos capas (defensa en profundidad)

El acceso a un dato debe superar **dos controles independientes**. Si uno fallara por un error de programación, el otro sigue en pie y no se exponen datos.

CAPA 1 · Aplicación

Cada consulta filtra explícitamente por el **origen del solicitante** (@Origen), que siempre proviene del credencial. No existe un parámetro de “tenant” que el cliente controle.

▼ y además ▼

CAPA 2 · Motor de base de datos (Row-Level Security)

La propia base de datos vuelve a filtrar cada fila por el tenant activo de la sesión. Aunque una consulta tuviera un error y “olvidara” filtrar, el motor **no devuelve ni deja insertar** filas de otro tenant. Cobertura actual: **44 de 44** tablas de RH.

POR QUÉ IMPORTA

El dato solo se libera si pasa las DOS capas. Es la diferencia entre "confiamos en que el código filtre bien" y "el motor lo impide aunque el código falle".

SECCIÓN 03

Cómo fluye la identidad del tenant

En cada petición, la identidad de la organización se establece del lado del servidor y viaja hasta el motor de datos:

1. **Petición entrante**
   Llega desde la app web, la API REST o un asistente de IA (MCP).
2. **Autenticación**
   Se valida la credencial: sesión SSO (JWT), API key o token OAuth.
3. **Se extrae el tenant**
   De la credencial se obtiene el **origen** — nunca del contenido que envía el cliente.
4. **Se fija el contexto seguro**
   El servidor establece el tenant activo en la conexión de base de datos (SESSION_CONTEXT).
5. **Capa 1 — filtro de aplicación**
   La consulta pide solo lo del **origen** del solicitante.
6. **Capa 2 — RLS del motor**
   La base de datos vuelve a filtrar y bloquea cualquier fila ajena.
7. **Resultado**
   Se devuelven únicamente los datos de la organización dueña.

SECCIÓN 04

Superficies de acceso y cómo se aíslan

Todas las vías de acceso comparten el **mismo** mecanismo de tenant descrito arriba. Las integraciones para terceros y para IA son de **solo lectura**.

Superficie	Autenticación	Cómo se aísla
App web colaborador / RH	Sesión SSO (JWT OpenIddict)	Identidad → origen → las 2 capas
API REST /api/ext	API key (rsk_..., hash SHA-256)	Mismo mecanismo · solo lectura
Servidor MCP asistentes de IA	API key u OAuth 2.1 (PKCE)	Mismo mecanismo · solo lectura
Webhooks salientes	Firma HMAC-SHA256 por tenant	Cada evento se entrega solo al webhook de su propio tenant

SECCIÓN 05

Verificación empírica (no solo teoría)

Probamos el aislamiento directamente contra la base de datos de producción, forzando el contexto de tenant en el motor y contando filas visibles en las tablas de RH (cursos, comunicados, NOM-035, RIT, descansos, API keys, etc.):

Escenario	Qué representa	Resultado
Contexto = tenant ajeno	Un tercero intentando leer datos que no son suyos	**0 filas en TODAS las tablas — bloqueado**
Contexto = tenant real	La organización dueña de los datos	Ve únicamente **sus propios** datos
Procesos internos	Tareas de sistema (envíos, mantenimiento) sin sesión de usuario	Operan con acceso controlado (fail-open seguro); no exponen datos a clientes

CONCLUSIÓN

Un tenant que no es el dueño ve cero. El aislamiento no depende de que “el código se porte bien”: lo impone el motor de base de datos.

SECCIÓN 06

Medidas de seguridad adicionales

IDENTIDAD Y ACCESO

Inicio de sesión propio (SSO OpenIddict) con contraseñas protegidas con BCrypt, **passkeys** (WebAuthn, sin contraseña), bloqueo por intentos fallidos, revocación de sesión en minutos y sesión deslizante.

TRANSPORTE Y SUPERFICIE

HTTPS forzado con HSTS, encabezados de seguridad OWASP + CSP, ocultamiento de la tecnología del servidor, y **límites de tasa** (rate limiting) por IP y por API key, con protección anti-enumeración en el kiosco del checador.

DATOS EN REPOSO Y SENSIBLES

Cifrado en reposo (TDE de Azure SQL); **cifrado a nivel de campo** (Always Encrypted) para los datos más sensibles del expediente; y **bitácora** de acceso a datos sensibles (quién vio o modificó qué).

INTEGRACIONES CONTROLADAS

API keys guardadas como hash y revocables al instante (solo lectura); OAuth 2.1 dedicado al asistente de IA —con PKCE, de solo lectura y **aislado** del SSO de la plataforma —; y webhooks **firmados** (HMAC) con reintentos.

ARCHIVOS Y MULTIMEDIA

Almacenamiento privado en Azure Blob con acceso mediante enlaces temporales de vida corta (SAS) e identidad administrada; sin URLs públicas permanentes.

DATOS BIOMÉTRICOS (verificación facial del checador)

Consentimiento **expreso y revocable** conforme a la LFPDPPP, y **purga automática** de las imágenes fuera de la ventana de retención.

SECCIÓN 07

Alineación con la LFPDPPP

Los datos de RH incluyen categorías **sensibles** (salud e incapacidades, biométricos, afiliación). La plataforma se diseñó alineada a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares: consentimiento expreso para datos sensibles, minimización y separación por organización, bitácora de accesos, cifrado de los campos críticos y retención/purga de biométricos.

Nota de honestidad: la determinación oficial de obligaciones —por ejemplo la prima de riesgo del IMSS— corresponde a la autoridad. RedSmart **registra y estima**, no sustituye al IMSS/SUA.

SECCIÓN 08

Glosario de términos

Término	Qué significa
Tenant	Cada organización cliente de la plataforma; sus datos están separados de los demás.
Origen	Etiqueta interna que marca a qué tenant pertenece cada dato.
RLS	Row-Level Security: filtrado por fila que aplica el propio motor de base de datos.
SSO	Inicio de sesión único; el sistema central de identidad de RedSmart.
MCP	Protocolo que permite a asistentes de IA consultar datos de forma estandarizada.
API key	Llave secreta (rsk_…) que autentica a un sistema tercero; de solo lectura y revocable.
OAuth 2.1 · PKCE	Estándar seguro para que apps como ChatGPT o Claude se conecten sin compartir contraseñas.
HMAC	Firma criptográfica que garantiza que un webhook viene de RedSmart y no fue alterado.
SAS	Enlace temporal a un archivo en almacenamiento; caduca por sí solo.
TDE · Always Encrypted	Cifrado en reposo (todo el disco) y cifrado a nivel de campo (datos puntuales).
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En resumen

Separación por diseño + dos capas independientes y **verificadas** + credenciales y transporte endurecidos + datos sensibles cifrados y auditados. RedSmart RH trata la información de tu gente como lo más crítico — porque lo es.

¿Dudas técnicas o revisión de seguridad?

Go4IT · RedSmart RH — con gusto ampliamos cualquier punto de este documento con tu equipo de TI o de cumplimiento.