SEGURIDAD Y PRIVACIDAD DE LOS DATOS EN VIGÍA SST

Resumen técnico de cómo se protegen, aíslan y respaldan los datos de tu Sistema de Gestión de Seguridad y Salud en el Trabajo — pensado para compartir con tu equipo de cumplimiento o con tus propios clientes.

Aislado
POR EMPRESA, SIN EXCEPCIÓN

Privado
ALMACENAMIENTO EN LA NUBE SIN ACCESO PÚBLICO

Trazable
BITÁCORA DE AUDITORÍA DE TODO CAMBIO

AISLAMIENTO DE DATOS MULTIEMPRESA

1 **Cada registro pertenece a una sola empresa**
Todas las tablas del sistema llevan la empresa propietaria del dato, y cada consulta a la base de datos se filtra automáticamente por la empresa activa de la sesión — a nivel de la capa de datos, no solo de la interfaz.

2 **Sin filtraciones entre empresas cliente**
Si administras varias empresas desde un portafolio, cada una ve exclusivamente su propia información: matriz de riesgos, trabajadores, incidentes, adjuntos.

ROLES Y PERMISOS REFORZADOS

3 **Verificación en cada solicitud**
Los roles (Administrador, Coordinador SST, COPASST, Trabajador) se validan en el servidor en cada acción — no basta con ocultar un botón en la pantalla.

4 **Principio de mínimo privilegio**
Cada rol ve y gestiona únicamente los módulos que le corresponden según su función real dentro del SG-SST.

ALMACENAMIENTO DE ARCHIVOS Y ADJUNTOS

5 **Bucket privado en la nube**
Actas, certificados, exámenes y demás soportes se guardan en almacenamiento de objetos en la nube (Cloudflare R2) configurado como privado — nunca existe una URL pública directa a un archivo.

6 **Entrega siempre autenticada**
Descargar un adjunto siempre pasa por el backend de la aplicación, que primero confirma que el usuario pertenece a la empresa dueña de ese archivo.

7 **Nombres de archivo no predecibles**
Cada archivo se guarda con un identificador único generado por el sistema, nunca con el nombre original — evita que alguien adivine o enumere rutas de archivos ajenos.

8 **Optimización sin exponer el original**
Imágenes y PDF se comprimen automáticamente al subir, reduciendo el costo de almacenamiento sin afectar la legibilidad del soporte.

CUENTAS, CONTRASEÑAS Y TRAZABILIDAD

9 Contraseñas nunca en texto plano

Se guardan como hash irreversible (bcrypt): ni el equipo técnico ni una filtración de la base de datos exponen la contraseña real de un usuario.

10 Bitácora de auditoría

Toda creación, modificación y eliminación queda registrada con usuario, fecha y detalle del cambio — con posibilidad de restaurar un registro eliminado por error.

11 Tráfico cifrado

Toda comunicación entre el navegador y la aplicación viaja cifrada mediante HTTPS/TLS.

12 Copias de seguridad antes de cambios mayores

Antes de cualquier actualización estructural de la base de datos se toma un respaldo completo, verificado antes de aplicar el cambio.

MARCO LEGAL

El tratamiento de datos personales dentro de Vigía SST se orienta a los principios de la Ley 1581 de 2012 (Régimen General de Protección de Datos Personales de Colombia): finalidad, seguridad, confidencialidad y acceso restringido a la información del titular.

QUÉ NO HACEMOS

PRÁCTICA	EN VIGÍA SST
Archivos en un bucket público	Nunca — todo adjunto exige autenticación y verificación de empresa.
Contraseñas en texto plano	Nunca — únicamente hash irreversible.
Consultas sin filtro de empresa	Nunca — el aislamiento aplica desde la capa de datos, no como capa opcional.
Borrado silencioso sin registro	Nunca — toda eliminación queda en la bitácora, con opción de restaurar.

Documento informativo, no constituye un informe de auditoría de seguridad certificado.