Red Smart

RedSmart RH - Seguridad y Privacidad

Cómo protegemos la información de tu gente, en todo momento.

La información de tu gente es de lo más sensible que existe

Nombres, CURP, RFC, NSS, datos de nómina, incidencias y hasta datos de salud. En RedSmart RH esa información está **protegida en todo momento** y su cuidado está diseñado **desde la base del sistema**, no como un añadido. Así lo hacemos:

Cómo protegemos la información

Cifrado en cada capa

Todo viaja cifrado (HTTPS/TLS) y se almacena cifrado. Los datos más sensibles —nómina, cuenta bancaria, NSS, salud— llevan cifrado **adicional a nivel de campo**, con llaves resguardadas en **Azure Key Vault**.

Acceso mínimo, por rol

Roles formales (administrador de marca, RH, colaborador): cada persona ve **sólo lo que le corresponde**. Los datos sensibles se muestran enmascarados salvo a quien está autorizado.

Identidad fuerte, sin contraseñas

Acceso con **llave de acceso (passkey)** y el bloqueo del dispositivo, sobre un inicio de sesión único (SSO) moderno.

Sesiones bajo control

Si das de baja o bloqueas a alguien, **pierde el acceso de inmediato**. Nada de sesiones que quedan abiertas para siempre.

Trazabilidad

Registramos **quién consulta o modifica** información sensible: para tu auditoría y para detectar cualquier uso indebido.

Nube confiable + respaldos

Sobre **Microsoft Azure** (Go4IT es Microsoft Partner), con alta disponibilidad y **respaldos cifrados**.

Cumplimos la Ley (LFPDPPP)

RedSmart RH está diseñado conforme a la **Ley Federal de Protección de Datos Personales en Posesión de los Particulares**:

- **Aviso de privacidad y consentimiento** — con consentimiento expreso para datos sensibles (salud, biométrico).
- **Derechos ARCO** — tus colaboradores pueden Acceder, Rectificar, Cancelar u Oponerse al uso de sus datos.
- **Retención y borrado seguro** — conservamos lo que la ley laboral exige y eliminamos de forma segura al concluir.

Aislamiento entre clientes: dos niveles, sin letra chica

- **Todos los planes:** tu información vive **aislada por marca en el propio motor de base de datos** (Row-Level Security): ningún otro cliente puede verla ni tocarla. El cifrado de campo usa **llaves de plataforma** custodiadas en Azure Key Vault.
- **Plan Enterprise:** para políticas corporativas o regulatorias que lo exijan, ofrecemos **base de datos dedicada con llaves de cifrado propias por cliente** ("tus datos, con tu llave").

Privacidad por diseño

- **Tu huella nunca sale del dispositivo.** El candado del dispositivo lo resuelve el propio equipo; RedSmart **no recibe ni almacena tu huella**. La selfie del registro se conserva un periodo configurable (90 días por omisión) y después se borra; la verificación facial (opcional) usa una **plantilla cifrada**, con consentimiento expreso.
- **Minimización.** Pedimos y guardamos **sólo lo necesario** para cumplir la ley y operar.
- **Tus datos son tuyos.** Exportables cuando quieras. RedSmart es marca blanca; **no comercializamos ni compartimos** la información de tu gente.

Microsoft Partner · Microsoft Azure · Cifrado en tránsito y en reposo · Aislamiento por marca (RLS) · Respaldos · Acceso por rol · Privacidad por diseño

Algunos controles se habilitan según la implementación y el plan contratado. Este documento describe nuestro enfoque de seguridad y privacidad y no constituye una certificación. Recomendamos validar el tratamiento de datos con tu asesor legal.