Cuestionario de seguridad

Respuestas al 28 de octubre de 2026. Para guardarlo, imprime esta página y elige «Guardar como PDF», o descarga el PDF. La explicación completa está en Seguridad; lo que Umbral se obliga a hacer, en los términos.

Si tu cuestionario tiene preguntas que no están aquí, escríbenos a seguridad@umbral-pld.com.

Empresa y alcance

Pregunta	Respuesta
¿Qué servicio presta Umbral?	Software como servicio para el cumplimiento de prevención de lavado de dinero (LFPIORPI): expedientes de clientes, enfoque basado en riesgos, avisos a la UIF, bitácora y reportes.
¿Qué papel tiene Umbral frente a los datos personales?	Umbral es persona encargada: trata los datos de los clientes finales por cuenta y bajo las instrucciones del cliente, que es el responsable (Anexo A de los términos).
¿Cuenta Umbral con certificaciones (ISO 27001, SOC 2)?	No por ahora. Este documento describe los controles que operan hoy; los centros de datos de los proveedores de infraestructura cuentan con sus propias certificaciones.
¿Se ha hecho una prueba de penetración externa?	Está planeada. Compartiremos el resumen ejecutivo con los clientes que lo soliciten cuando se realice.

Ubicación y proveedores

Pregunta	Respuesta
¿Dónde se guardan los datos?	En servidores y almacenamiento en Estados Unidos. La lista de proveedores, los datos que procesa cada uno y su ubicación están en el aviso de privacidad y en el Anexo A.3 de los términos.
¿Se usan subencargados?	Sí, para el servidor, el almacenamiento, el correo, los pagos, la facturación, la validación de identidad y la lectura de documentos. Se avisa con 30 días de anticipación antes de agregar uno nuevo.

Pregunta	Respuesta
¿Se usan los datos para entrenar inteligencia artificial?	No. El proveedor que lee documentos se comprometió por escrito a no usar los datos para entrenar sus modelos.

Cifrado y llaves

Pregunta	Respuesta
¿Los datos van cifrados en tránsito?	Sí. Toda conexión usa HTTPS. Los servidores solo reciben tráfico a través de una red de protección contra ataques; las conexiones directas se rechazan.
¿Los datos van cifrados en reposo?	Sí, en capas: la base de datos y los respaldos locales viven en un disco cifrado; la CURP, el RFC y los datos de la credencial para votar se cifran además dentro de la base (AES-256); los documentos se cifran (AES-256), con una llave propia de cada cliente, antes de salir de la aplicación; los respaldos se cifran (AES-256).
¿Cómo se busca un cliente si su CURP está cifrada?	Con una huella irreversible del dato (HMAC-SHA256 con una llave aparte), no con el dato.
¿Dónde están las llaves?	Fuera de la base de datos y del código. Una copia se guarda cifrada fuera del servidor; solo la puede abrir la persona responsable de la seguridad de Umbral.
¿Se rotan las llaves?	Sí, cada mes de forma automática: llaves de cifrado, firma de sesiones, frase de los respaldos, contraseñas de la base de datos y llave del disco. Lo que se puede volver a cifrar se cifra con la llave nueva.

Acceso y autenticación

Pregunta	Respuesta
¿Cómo se guardan las contraseñas?	No se guardan: se guarda una huella con sal y 100,000 iteraciones (PBKDF2 con SHA-512).

Pregunta	Respuesta
¿Hay verificación en dos pasos?	Sí, con aplicación autenticadora. El cliente puede hacerla obligatoria para todos sus usuarios; para el personal de Umbral es obligatoria siempre.
¿Qué pasa con los intentos fallidos?	La cuenta se bloquea por un tiempo tras varios intentos fallidos. Las olas de intentos fallidos generan una alerta al equipo de seguridad.
¿Hay control de acceso por roles?	Sí: roles (oficial de cumplimiento, capturista, auditor, entre otros) y permisos por sucursal.
¿Cuánto dura una sesión?	Ocho horas. Al cambiar la contraseña se cierran las demás sesiones.
¿Quién de Umbral tiene acceso a producción?	Solo el personal técnico autorizado, con llave criptográfica (nunca contraseña) y verificación en dos pasos en las cuentas de administración.

Separación de datos e integridad

Pregunta	Respuesta
¿Cómo se separan los datos de cada cliente?	Cada consulta a la base de datos se filtra por la empresa de quien la hace; ningún usuario ve datos de otra empresa. Las pruebas automáticas lo comprueban antes de cada cambio.
¿Hay bitácora de actividad?	Sí: altas, cambios (con valor anterior y nuevo), consultas de información sensible, descargas y accesos, con usuario, fecha y dirección IP. La ven el oficial de cumplimiento y el auditor del cliente, y se descarga en Excel.
¿Se puede alterar la bitácora?	La aplicación no tiene permiso de base de datos para modificarla ni borrarla. Además, cada registro va sellado con el anterior: un cambio, borrado o registro agregado directo en la base rompe la cadena, lo que se comprueba desde la aplicación y cada hora de forma automática.

Respaldos y continuidad

Pregunta	Respuesta
¿Con qué frecuencia se respalda?	Respaldo completo diario y respaldo de los cambios cada hora (pérdida máxima: una hora de trabajo).
¿Dónde se guardan los respaldos?	En el servidor (disco cifrado) y fuera de él, en almacenamiento que impide borrarlos durante los primeros 30 días; se conservan 90 días.
¿Se prueban los respaldos?	Sí, cada semana se restaura automáticamente el más reciente en una base aparte, se revisa su integridad y se mide el tiempo; si falla, el equipo recibe una alerta.
¿Se monitorea la disponibilidad?	Sí, de forma continua, con alertas al equipo.

Operación y desarrollo

Pregunta	Respuesta
¿Cómo se aplican parches de seguridad?	Las actualizaciones de seguridad del sistema operativo se instalan solas; cada semana se reconstruye la aplicación con las imágenes base más recientes.
¿Se revisan vulnerabilidades?	Sí: las librerías de la aplicación cada día y los contenedores cada semana, contra las listas públicas de vulnerabilidades conocidas.
¿Se revisan los archivos en busca de virus?	Sí. Cada archivo que se sube (también los que mandan los clientes finales desde su enlace) pasa por un antivirus antes de guardarse; uno con virus se rechaza y el equipo recibe una alerta. La base de virus se actualiza sola cada 2 horas y hay alerta si se atrasa o si el antivirus no responde (en ese caso el archivo no se guarda sin revisar).
¿Cómo llegan los cambios a producción?	Solo si pasan las pruebas automáticas y vienen firmados con la llave del equipo de Umbral; el servidor rechaza código sin firma. Si un despliegue falla, regresa solo a la versión anterior.
¿Cómo se protege el servidor?	Cortafuegos que solo admite tráfico web desde la red de protección, acceso administrativo solo con llave, bloqueo automático de intentos repetidos y alertas de fallas.

Incidentes y fin del contrato

Pregunta	Respuesta
¿Cómo se avisa un incidente?	Si una vulneración de seguridad afecta los datos del cliente, Umbral le avisa en un máximo de 72 horas desde que la detecta, con lo que se sepa y las medidas tomadas (Anexo A.2 de los términos).
¿Dónde se reportan vulnerabilidades?	En seguridad@umbral-pld.com (publicado también en security.txt). Respondemos en un día hábil.
¿Qué pasa con los datos al terminar el contrato?	El cliente tiene 60 días para descargarlos (o puede contratar custodia de solo consulta). Después Umbral los borra, junto con la llave de sus documentos (lo que quede en copias protegidas contra borrado ya no se puede abrir), y lo confirma por escrito (cláusula 14 de los términos). La obligación de conservar 10 años es del cliente.

Consulta también: Seguridad · Términos y condiciones · Aviso de privacidad.