



EDILIA TECH S.L.

CIF B-27552728

EXPEDIENTE DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

CATEGORÍA BÁSICA

Real Decreto 311/2022, de 3 de mayo

Sistema: Edilia (Copiloto), plataforma SaaS para la Administración Local

Dominio: edilia.tech y subdominios (copiloto.edilia.tech, admin.edilia.tech)

Versión 1.2, sustituye a la versión firmada el 12 de mayo de 2026

Fecha de aprobación: la de la firma electrónica de este documento



Contenido y cambios respecto a la versión anterior

Este expediente contiene cuatro documentos: (1) Política de Seguridad de la Información, (2) Designación del Responsable de Seguridad de la Información, (3) Plan de Continuidad del Servicio y (4) Declaración de Conformidad ENS Categoría Básica. Los cuatro se aprueban y firman de forma conjunta en este único fichero.

La versión 1.2 corrige la versión aprobada el 12 de mayo de 2026 para que refleje el sistema tal como está hoy:

Apartado	Versión anterior	Versión 1.2
Dominio del sistema	ayto.app y subdominios	edilia.tech y subdominios (el dominio ayto.app ya no se utiliza)
Correo de seguridad y de protección de datos	seguridad@ayto.app, dpd@ayto.app	contacto@edilia.tech
Concentración de roles	Justificada por el tamaño de la sociedad	Justificada y con medidas compensatorias expresas (art. 13 del RD 311/2022)
Copias de seguridad	Ruta y retención de 30 días no vigentes	Mecanismos y retenciones reales comprobados el 19/09/2026
Pruebas de restauración	Trimestrales	Anuales; la primera se realizó el 19/09/2026
Respaldo del modelo de IA	Anthropic API	Amazon Bedrock en la Unión Europea
Servidor de aplicaciones	PHP-FPM 8.3	PHP-FPM 8.4
Acceso remoto por SSH	Puerto no estándar 2222	Referencia eliminada: el servicio usa el puerto 22 con clave pública y fail2ban
Autoevaluación	19 medidas, marzo de 2026	Se añade la revisión ampliada del 19/09/2026 y un plan de mejora



DOCUMENTO 1

Política de Seguridad de la Información

Edilia Tech S.L. · Sistema Edilia (edilia.tech)

1. Objeto y ámbito

La presente Política de Seguridad de la Información (en adelante, PSI) establece el marco de referencia para la protección de los activos de información de Edilia Tech S.L. en la prestación del servicio Edilia, plataforma SaaS dirigida a las Administraciones Públicas Locales españolas para la generación asistida de documentos administrativos.

Esta política se aprueba en cumplimiento de las medidas org.1 y org.2 del Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), y resulta de aplicación a la totalidad del personal, infraestructura, sistemas y servicios de Edilia Tech S.L. incluidos en el sistema Edilia.

2. Marco normativo de referencia

- a) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- b) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- c) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- d) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD), y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- e) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, sobre Inteligencia Artificial (AI Act).
- f) Guías CCN-STIC, en particular la CCN-STIC 803 (valoración), CCN-STIC 804 (implantación), CCN-STIC 809 (declaración y certificación de conformidad) y CCN-STIC 890A (perfil de cumplimiento ENS Básico).

3. Misión y compromiso de la dirección

Edilia Tech S.L. asume el compromiso institucional con la seguridad de la información de sus clientes públicos y de los datos que estos le confían. La dirección reconoce que la confianza de las Administraciones Públicas en la plataforma Edilia depende de la solidez de las medidas de seguridad implantadas y de la transparencia con la que estas se documentan. Este compromiso se traduce en:

- a) Asignación de recursos económicos, humanos y tecnológicos suficientes para la seguridad de la información, en proporción a la capacidad de la sociedad.



- b) Aprobación, revisión anual y, en su caso, actualización de esta política.
- c) Difusión de la política a todo el personal con acceso a los sistemas.
- d) Adopción de un enfoque de mejora continua basado en análisis de riesgos.

4. Principios rectores

La seguridad de la información en Edilia Tech S.L. se rige por los siguientes principios, conforme al artículo 5 del RD 311/2022:

- a) Seguridad como proceso integral. La seguridad se contempla en todas las fases del ciclo de vida del servicio, desde el diseño hasta la retirada.
- b) Gestión de la seguridad basada en los riesgos. Las medidas se adoptan en función del análisis de riesgos del sistema y de su categoría ENS.
- c) Prevención, detección, respuesta y conservación. Se combinan medidas anticipativas con capacidades de detección, contención y recuperación.
- d) Existencia de líneas de defensa. Se implementan controles en distintos niveles (red, sistema, aplicación, datos) para garantizar la defensa en profundidad.
- e) Vigilancia continua. Se monitorizan los sistemas mediante registro de actividad, captación de eventos de seguridad y alertas automáticas.
- f) Reevaluación periódica. Las medidas se revisan al menos anualmente y siempre que se produzcan cambios significativos en el sistema.
- g) Diferenciación de responsabilidades. Los roles se mantienen identificados conforme al apartado 5 de esta política. Su concentración en una misma persona es temporal y excepcional y se compensa con las medidas recogidas en el Documento 2.

5. Estructura organizativa de seguridad

5.1. Responsable de la Información. Recae en D. Roberto López Miquel, en su condición de administrador único de Edilia Tech S.L., como máximo responsable de los activos de información del sistema Edilia y del corpus jurídico-administrativo que alimenta la plataforma. Determina los requisitos de la información en términos de confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad.

5.2. Responsable del Servicio. Recae en D. Roberto López Miquel, en su condición de administrador único, responsable de la prestación efectiva del servicio Edilia a las entidades públicas clientes y de la relación contractual con estas.

5.3. Responsable de Seguridad de la Información (RSI). Recae en D. Roberto López Miquel, conforme a la designación formal recogida en el Documento 2. Sus funciones se desarrollan en dicho documento. La concentración de este rol con los de Responsable de la Información y Responsable del Servicio, y con la administración técnica del sistema, se debe a que la sociedad no dispone hoy de recursos para separarlos. Es temporal y se compensa con las medidas del Documento 2. Se separarán los roles a más tardar cuando



se formalice la ampliación de capital de la sociedad.

5.4. Punto de contacto. El punto de contacto para asuntos de seguridad de la información y de protección de datos personales es contacto@edilia.tech.

6. Gestión de riesgos

La gestión de riesgos se realizará conforme a la metodología MAGERIT v3 promovida por el CCN. El análisis de riesgos se documenta y revisa al menos con periodicidad anual, así como ante cualquier cambio significativo en el sistema. La herramienta de referencia es PILAR, distribuida por el CCN-CERT. Las decisiones sobre tratamiento de riesgos (aceptación, mitigación, transferencia o eliminación) se documentan formalmente y se elevan al Responsable de Seguridad para su aprobación.

7. Datos personales

Edilia Tech S.L. trata datos personales únicamente como encargado del tratamiento (art. 28 RGPD) por cuenta de las entidades públicas clientes, que conservan la condición de responsables del tratamiento. La cadena completa de subencargados se documenta en el contrato de encargado del tratamiento que se firma con cada cliente.

Toda la cadena de procesamiento de IA se ejecuta en territorio de la Unión Europea: el modelo lingüístico principal se aloja en Vertex AI en la Unión Europea, con respaldo en Amazon Bedrock en la región de Fráncfort (eu-central-1), y el motor de embeddings semánticos se ejecuta en infraestructura de Mistral AI con sede en Francia. No se realizan transferencias internacionales de datos a terceros países fuera del Espacio Económico Europeo.

8. Categorización del sistema

El sistema Edilia ha sido categorizado conforme al Anexo I del RD 311/2022 atendiendo a las cinco dimensiones de seguridad de los activos del sistema. La valoración resultante sitúa al sistema en categoría Básica, conforme al detalle recogido en el Documento 4.

9. Obligaciones del personal

Todo el personal con acceso a los sistemas de Edilia Tech S.L. está obligado a:

- a) Conocer y respetar la presente política y la normativa interna de seguridad.
- b) Utilizar credenciales individuales y no compartirlas.
- c) Comunicar al Responsable de Seguridad cualquier incidente, anomalía o sospecha de compromiso.
- d) Aplicar el principio de mínimo privilegio en su trabajo diario.
- e) Mantener la confidencialidad de la información a la que accedan, incluso tras la finalización de su relación con la sociedad.



10. Gestión de incidentes

Edilia Tech S.L. dispone de un procedimiento de gestión de incidentes de seguridad que contempla la detección, contención, erradicación, recuperación y lecciones aprendidas. En caso de incidente que afecte a datos personales, se aplicará el procedimiento de notificación de brecha conforme al artículo 33 RGPD, en plazo no superior a setenta y dos horas desde su conocimiento. Los incidentes que afecten a sistemas de Administraciones Públicas clientes podrán ser notificados al CCN-CERT conforme a lo previsto en la Instrucción Técnica de Seguridad de notificación de incidentes.

11. Revisión y aprobación

La presente política será revisada al menos con periodicidad anual y siempre que se produzcan cambios significativos en el sistema, en la organización o en el marco normativo aplicable. Las revisiones se documentarán mediante actualización de la versión del documento y su correspondiente aprobación formal. La próxima revisión ordinaria será en mayo de 2027.

12. Aprobación

La presente Política de Seguridad de la Información se aprueba en Madrid, en la fecha de la firma electrónica que consta en este documento, por el administrador único de Edilia Tech S.L.

D. Roberto López Miquel
Administrador único
Edilia Tech S.L. · CIF B-27552728



DOCUMENTO 2

Designación del Responsable de Seguridad de la Información

Antecedentes

El artículo 13 del Real Decreto 311/2022 obliga a las entidades sujetas al ENS a designar formalmente a las personas físicas que asumen los roles de Responsable de la Información, Responsable del Servicio y Responsable de Seguridad de la Información. La Política de Seguridad de la Información de Edilia Tech S.L., aprobada en la misma fecha que el presente documento, requiere completar esta designación mediante acto formal.

Designación

Edilia Tech S.L., con CIF B-27552728, en uso de las facultades que le confieren los estatutos sociales y dada su condición de micro-empresa, DESIGNA formalmente como Responsable de Seguridad de la Información de la sociedad y del sistema Edilia a:

D. Roberto López Miquel

Administrador único de Edilia Tech S.L.

Justificación de la concentración de roles y medidas compensatorias

Edilia Tech S.L. mantiene en D. Roberto López Miquel los roles de Responsable de la Información, Responsable del Servicio y Responsable de Seguridad de la Información, y la administración técnica del sistema recae en la misma sociedad sin plantilla diferenciada. Esta concentración es temporal y excepcional: los recursos actuales de la sociedad no permiten separar la responsabilidad de seguridad de la explotación del sistema.

Conforme al principio de diferenciación de responsabilidades del RD 311/2022, se aplican las siguientes medidas compensatorias:

- a) El registro de auditoría del sistema permite distinguir las actuaciones realizadas en cada rol.
- b) Los cambios de seguridad relevantes (accesos, cortafuegos, copias de seguridad, claves) se documentan por escrito antes de aplicarse.
- c) El Responsable de Seguridad realiza una revisión anual del sistema con una lista de comprobación documentada. En cuanto la sociedad disponga de financiación, esa revisión la realizará un tercero independiente.
- d) Esta designación se revisará y los roles se separarán a más tardar cuando se formalice la ampliación de capital de la sociedad.



Funciones del Responsable de Seguridad

El Responsable de Seguridad de la Información asume, conforme al artículo 13 del RD 311/2022, las siguientes funciones:

- a) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, en sus dimensiones de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- b) Realizar o promover las autoevaluaciones o auditorías periódicas que permitan verificar el cumplimiento de los requisitos del ENS.
- c) Promover la formación y concienciación en materia de seguridad de la información.
- d) Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- e) Analizar, completar y aprobar la documentación de seguridad del sistema.
- f) Supervisar la atención y respuesta a los incidentes de seguridad.
- g) Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del RD 311/2022.
- h) Determinar las medidas de seguridad que deben aplicarse, según lo previsto en el Anexo II del RD 311/2022.

Vigencia

La presente designación tiene carácter indefinido y permanecerá vigente hasta su revocación expresa o hasta que cese la condición que motiva su nombramiento. Cualquier modificación se documentará mediante nueva resolución.

Aceptación y firma

D. Roberto López Miquel, en calidad de administrador único de Edilia Tech S.L., aprueba la presente designación y acepta personalmente el cargo de Responsable de Seguridad de la Información, comprometiéndose a desempeñarlo conforme a las funciones descritas, a la Política de Seguridad de la Información aprobada y al marco normativo vigente. En Madrid, en la fecha de la firma electrónica que consta en este documento.

D. Roberto López Miquel

Administrador único y Responsable de Seguridad de la Información

Edilia Tech S.L. · CIF B-27552728



DOCUMENTO 3

Plan de Continuidad del Servicio

Sistema Edilia (edilia.tech)

1. Objeto

El presente Plan de Continuidad del Servicio (en adelante, PCS) establece las medidas, procedimientos y responsabilidades necesarias para garantizar la recuperación del servicio Edilia en caso de incidente grave, conforme a la medida op.cont.2 del Anexo II del Real Decreto 311/2022. El PCS resulta de aplicación a la totalidad de la infraestructura productiva de Edilia Tech S.L. incluida en el sistema Edilia y se complementa con la Política de Seguridad de la Información aprobada por la sociedad.

2. Alcance del servicio

El servicio cubierto por este plan comprende la plataforma SaaS Edilia, accesible a través de los siguientes subdominios de edilia.tech: copiloto.edilia.tech (Copiloto, para personal técnico municipal) y admin.edilia.tech (panel de administración). No incluye el producto Compliance, que es un sistema distinto. La infraestructura productiva está alojada en un servidor virtual privado del proveedor IONOS, dentro del territorio de la Unión Europea, e incluye los componentes Nginx, PHP-FPM 8.4, MySQL 8, PostgreSQL con extensión pgvector, Redis, Horizon y Supervisor.

3. Análisis de Impacto en el Negocio (BIA)

Para el sistema Edilia, considerado como servicio de apoyo a la actividad ordinaria de las entidades públicas clientes, no esencial 24/7 pero relevante en horario laboral, se establecen los siguientes objetivos:

Parámetro	Valor objetivo	Justificación
RTO (tiempo de recuperación)	8 horas	Restablecimiento del servicio en jornada laboral siguiente al incidente.
RPO (punto de recuperación)	24 horas	Copias diarias automatizadas. Pérdida máxima admisible: trabajo de un día.
MTPD (período máximo)	72 horas	Más allá comprometería confianza institucional y obligaciones contractuales con AAPP.

Los valores son objetivos de diseño. La primera prueba de restauración parcial (ver apartado 7) tardó 26 segundos para la base de datos MySQL, muy por debajo del RTO; falta medir la restauración completa del servidor.

4. Estrategia de copias de seguridad

Edilia Tech S.L. mantiene los siguientes mecanismos de copia de seguridad sobre la infraestructura productiva:

- a) Volcados de las bases de datos MySQL y PostgreSQL cada día a las 00:45, con copias incrementales adicionales a las 15:00 y a las 22:00. Se conservan localmente los tres más recientes, en un directorio accesible únicamente por el administrador del sistema.
- b) Copia diaria a las 02:00 de las aplicaciones y sus bases de datos, cifrada con GPG (AES-256), con retención de 7 días en el servidor y de 14 días en un almacenamiento externo en la nube.
- c) Imagen completa diaria del servidor mediante el servicio de copias del proveedor IONOS (Acronis), con la retención que fija el contrato con el proveedor.
- d) Pruebas de restauración: al menos una prueba anual documentada, sobre una base de datos auxiliar y nunca sobre producción. La primera se realizó el 19 de septiembre de 2026 (ver apartado 7). Su resultado se registra en el registro de auditoría.

5. Procedimiento de recuperación

5.1. Detección y notificación (0 a 30 minutos). La detección puede producirse por monitorización activa (Sentry, alertas de salud), notificación de cliente o detección interna. Cualquier incidente debe notificarse de inmediato al Responsable de Seguridad.

5.2. Evaluación inicial (30 minutos a 2 horas). El Responsable de Seguridad evalúa la naturaleza del incidente, su gravedad, los servicios afectados y la conveniencia de activar el presente plan.

5.3. Recuperación técnica (2 a 8 horas). a) Aislamiento del componente afectado si procede. b) Identificación de la última copia de seguridad íntegra disponible. c) Restauración sobre infraestructura limpia. d) Verificación de integridad de los datos restaurados. e) Verificación de servicios críticos (autenticación, generación de documentos, firma). f) Restablecimiento del acceso a usuarios.

5.4. Comunicación a clientes (continuo). Durante la incidencia se mantendrá informados a los responsables designados por cada entidad pública cliente afectada, mediante correo electrónico y, si procede, mediante actualización del estado en una página de incidencias.

5.5. Cierre y lecciones aprendidas (24 a 72 horas). El Responsable de Seguridad redactará un informe post-incidente con cronología, causas raíz, impacto observado, medidas adoptadas y propuestas de mejora, que se archivará y se incorporará a la siguiente revisión del análisis de riesgos.



6. Escenarios contemplados

Escenario	Respuesta primaria	Respuesta secundaria
Caída temporal del VPS	Reinicio supervisado y diagnóstico con Sentry.	Reaprovisionamiento desde la imagen del proveedor.
Corrupción de base de datos	Restauración desde la copia diaria más reciente.	Restauración desde una copia anterior de la retención disponible.
Compromiso de credenciales	Rotación inmediata de credenciales afectadas y cierre forzado de sesiones.	Notificación a clientes afectados y, si procede, brecha RGPD.
Indisponibilidad de Vertex AI	Respaldo automático en Amazon Bedrock en la Unión Europea.	Modo degradado: edición manual sin asistencia de IA.
Cifrado por ransomware	Aislamiento del servidor y restauración desde la copia cifrada externa.	Reaprovisionamiento completo en infraestructura limpia.

7. Pruebas y mantenimiento

Este plan se prueba al menos con periodicidad anual mediante simulación documentada de al menos un escenario crítico (típicamente, restauración completa de base de datos sobre infraestructura limpia). La primera prueba se realizó el 19 de septiembre de 2026: se restauró el último volcado de la base de datos MySQL del sistema (70 MB, generado a las 15:00) en una base auxiliar, sin tocar producción. Tardó 26 segundos, recuperó las 181 tablas y los recuentos de las tablas comprobadas coincidieron con la base real (las diferencias se debían a la actividad posterior al volcado). Queda pendiente probar la restauración de la base PostgreSQL (legislación) y de la imagen completa del servidor, antes del 31 de diciembre de 2026. Los resultados se registran y, si revelan deficiencias, se incorporan al ciclo de mejora. El plan se revisa al menos anualmente y siempre que se produzcan cambios significativos en la infraestructura, en los servicios prestados o en la estructura organizativa de Edilia Tech S.L.

8. Aprobación

El presente Plan de Continuidad del Servicio se aprueba en Madrid, en la fecha de la firma electrónica que consta en este documento.

D. Roberto López Miquel

Administrador único y Responsable de Seguridad de la Información

Edilia Tech S.L. · CIF B-27552728



DOCUMENTO 4

Declaración de Conformidad ENS

Categoría Básica

Real Decreto 311/2022, de 3 de mayo

1. Identificación del declarante

Razón social	Edilia Tech S.L.
CIF	B-27552728
Representante	D. Roberto López Miquel (administrador único)
Responsable de Seguridad	D. Roberto López Miquel (rol concentrado con medidas compensatorias, ver Documento 2)
Correo de seguridad y de protección de datos	contacto@edilia.tech

2. Identificación del sistema

Denominación del sistema	Edilia (Copiloto)
Naturaleza	Plataforma SaaS de generación asistida por IA de documentos administrativos para Administraciones Públicas Locales.
Dominio técnico	edilia.tech y subdominios (copiloto.edilia.tech, admin.edilia.tech)
Versión del expediente	1.2
Ubicación de la infraestructura	VPS del proveedor IONOS, territorio de la Unión Europea.

3. Categorización del sistema

Conforme al Anexo I del RD 311/2022, se ha realizado la valoración de los activos del sistema atendiendo a las cinco dimensiones de seguridad. El resultado es el siguiente:

Dimensión	Nivel	Justificación
Confidencialidad (C)	BAJO	El sistema no procesa datos de categorías especiales del art. 9 RGPD de forma sistemática. La información tratada es administrativa ordinaria. Esta valoración se someterá a la validación de un consultor ENS externo en cuanto la sociedad disponga de financiación.
Integridad (I)	BAJO	La integridad final del documento corresponde al técnico municipal que



lo firma. Edilia es herramienta de apoyo, no firma actos administrativos.

Disponibilidad (D)	BAJO	Servicio no esencial 24/7. RTO de 8 horas admisible para la naturaleza de apoyo a la actividad ordinaria.
Autenticidad (A)	BAJO	Autenticación con contraseñas cifradas (bcrypt) y sesiones cifradas. La firma legal corresponde al técnico, no al sistema.
Trazabilidad (T)	BAJO	Sistema de auditoría con registro de los eventos críticos. El sistema de fe pública es el del ayuntamiento.

Categoría resultante del sistema: **BÁSICA**. Cuando el sistema integre operativamente el módulo de Canal de Denuncias o el módulo de RRHH municipal con datos disciplinarios, se procederá a una recategorización al alza hacia la categoría MEDIA.

4. Autoevaluación de las medidas del Anexo II

Se ha realizado una autoevaluación técnica documentada de las medidas del Anexo II del RD 311/2022, con análisis de evidencias en código y configuración del sistema.

a) Autoevaluación del 27 de marzo de 2026 (19 medidas aplicables): 3 medidas cumplidas y 16 parcialmente implantadas (marco organizativo 0 de 3, marco operacional 1 de 8, medidas de protección 2 de 8). Tras la aprobación de la política de seguridad, la designación del Responsable y el plan de continuidad, las medidas org.1, org.3 y op.cont.2 pasan a estar cumplidas.

b) Revisión ampliada del 19 de septiembre de 2026: se examinaron 64 controles, evaluados contra los requisitos de la categoría Media, más exigentes que los de la Básica. La conclusión es que la mayoría de los controles están implantados de forma parcial y que existen brechas por cerrar.

c) Plan de mejora, por orden de prioridad: (1) completar las pruebas de restauración (PostgreSQL e imagen completa del servidor) antes del 31 de diciembre de 2026, ya realizada la de MySQL; (2) endurecimiento del acceso remoto (desactivar la autenticación por contraseña en SSH y acotar los privilegios de administración); (3) autenticación multifactor en el panel de administración; (4) monitorización y alertas de seguridad; (5) formalizar el análisis de riesgos MAGERIT y la relación con los proveedores.

d) La autoevaluación se repetirá al menos cada dos años y siempre que haya cambios significativos, conforme a la Guía CCN-STIC 809.

5. Evidencias técnicas implementadas

Las evidencias a), i), j), o) y p) se verificaron el 19 de septiembre de 2026. Las evidencias b) a h) y k) a n) proceden de la auditoría técnica del 27 de marzo de 2026.

a) Cifrado en tránsito mediante TLS 1.2 o superior, con HTTPS forzado y cabecera HSTS,



y rechazo de TLS 1.0 y 1.1.

- b) Cifrado de cookies de sesión y almacenamiento en Redis cifrado.
- c) Algoritmo de hash de contraseñas bcrypt con factor de coste 12.
- d) Política de contraseñas: mínimo 10 caracteres, letras, números y combinación de mayúsculas y minúsculas.
- e) Registro de auditoría con los eventos críticos del sistema.
- f) Pseudonimización de IP, correo y nombre en los registros de auditoría.
- g) Pseudonimización del correo en la captura de errores Sentry, ubicado en región UE.
- h) Aislamiento multi-tenant por municipio en controladores críticos.
- i) Acceso a las bases de datos restringido a la interfaz de bucle local.
- j) Cortafuegos con denegación de entrada por defecto (solo puertos web y de administración), acceso SSH con clave pública y protección fail2ban.
- k) Limitación de peticiones (throttling) en rutas críticas (contacto, salud, chatbot, firma).
- l) Detección de anomalías de IP en el inicio de sesión, con notificación a administradores.
- m) Filtrado anti prompt-injection en las llamadas al modelo de lenguaje.
- n) Verificación obligatoria de correo electrónico.
- o) Copias de seguridad diarias cifradas con GPG y copia externa (ver Documento 3).
- p) Instalación automática de las actualizaciones de seguridad del sistema operativo.

6. Tratamiento de datos personales

Edilia Tech S.L. actúa exclusivamente como encargado del tratamiento (art. 28 RGPD) por cuenta de las entidades públicas clientes. Toda la cadena de procesamiento se ejecuta en territorio de la Unión Europea. No se realizan transferencias internacionales a terceros países fuera del Espacio Económico Europeo. La política de privacidad se publica en el dominio del servicio y se firma un contrato de encargado del tratamiento individualizado con cada entidad cliente.

7. Declaración

D. Roberto López Miquel, en calidad de administrador único de Edilia Tech S.L., con CIF B-27552728, en virtud de las facultades que tiene conferidas, DECLARA bajo su responsabilidad que el sistema Edilia, identificado en el apartado 2 del presente documento, se adecúa a los principios y requisitos del Esquema Nacional de Seguridad establecidos en el Real Decreto 311/2022, de 3 de mayo, en su categoría BÁSICA, conforme a la autoevaluación documentada y con el plan de mejora recogido en el apartado 4.

La presente declaración se realiza al amparo de lo previsto en la disposición adicional segunda del citado Real Decreto, que permite a las entidades del sector privado que prestan servicios o suministran soluciones a las entidades del sector público acreditar el cumplimiento del ENS para los sistemas que prestan dichos servicios. Edilia Tech S.L. se



compromete a mantener actualizado el expediente de adecuación y a someterse a las auditorías que sean preceptivas conforme avance la categoría del sistema.

8. Vigencia y publicación

La presente declaración de conformidad tiene una vigencia de dos años desde su firma, sin perjuicio de su revisión anticipada en caso de cambios significativos en el sistema. Una copia de esta declaración está disponible para consulta de las entidades públicas clientes en <https://edilia.tech/legal/declaracion-conformidad-ens>.

9. Firma

En Madrid, en la fecha de la firma electrónica que consta en este documento.

D. Roberto López Miquel

Administrador único y Responsable de Seguridad de la Información

Edilia Tech S.L. · CIF B-27552728

Firmado por ***2256** ROBERTO LOPEZ (R:
****5272*) el día 19/09/2026 con un
certificado emitido por AC Representación