5Tech Platform — Guía del usuario

Guía del usuario · `sensorium-platform-manual` · Borrador de revisión (preliminar, PROPUESTO) · 2026-07-18 · Estado: Preliminar

> **PRELIMINAR — VALORES PROPUESTOS.** Esta guía describe la funcionalidad prevista de la 5Tech Platform. Los valores marcados con ‡ son cifras propuestas, típicas del sector (suites de seguridad, periodos de retención, objetivos de SLA, versiones de navegador, cadencias), incluidos para que ningún elemento quede en blanco. **No son definitivos ni contractuales**; se confirman como parte del despliegue y pueden cambiar. Las etiquetas exactas de las pantallas, la navegación y los nombres de los roles están sujetos a cambios. Un `[TBD]` restante marca un término legal/contractual (garantía/licencia) que no debe inventarse. Consulte §13 para los términos del servicio.

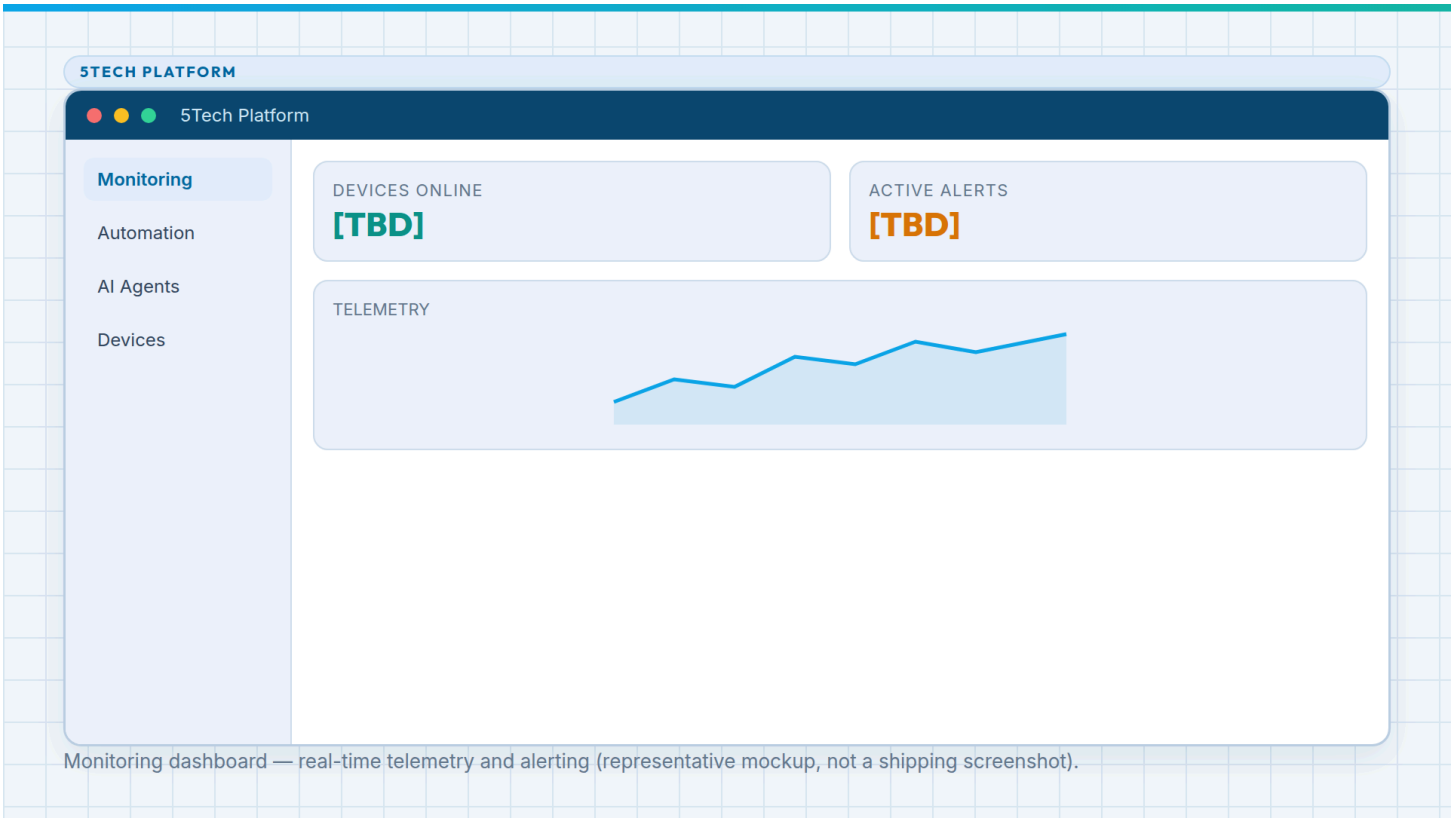

Figura FIG-001 — El panel de monitoreo de la 5Tech Platform: telemetría en vivo, KPI y alertas activas.

1. Descripción general y conceptos

1.1 Qué es la 5Tech Platform

La **5Tech Platform** es el software —la capa *Decide*— del ecosistema 5Tech. Convierte los datos de campo en monitoreo, alertas y acción con intervención humana. El propósito de 5Tech es *«cerrar la brecha entre las operaciones físicas complejas y la inteligencia digital»*, con la auditabilidad que requieren las empresas industriales. La Plataforma es donde esos datos se vuelven útiles.

Recibe telemetría del **Sensorium™ Gateway** —la capa *Connect* que agrega dispositivos de campo como los sensores Zone Awareness y los módulos SmartBolt por BLE y la publica por MQTT— y la presenta a través de tres capas de trabajo: **Monitoreo**, **Automatización** y **Asistencia de IA**. Puede integrarse con sus sistemas **SCADA** y **ERP** existentes para que las decisiones que toman las personas puedan impulsar acciones operativas reales.

1.2 Las tres capas

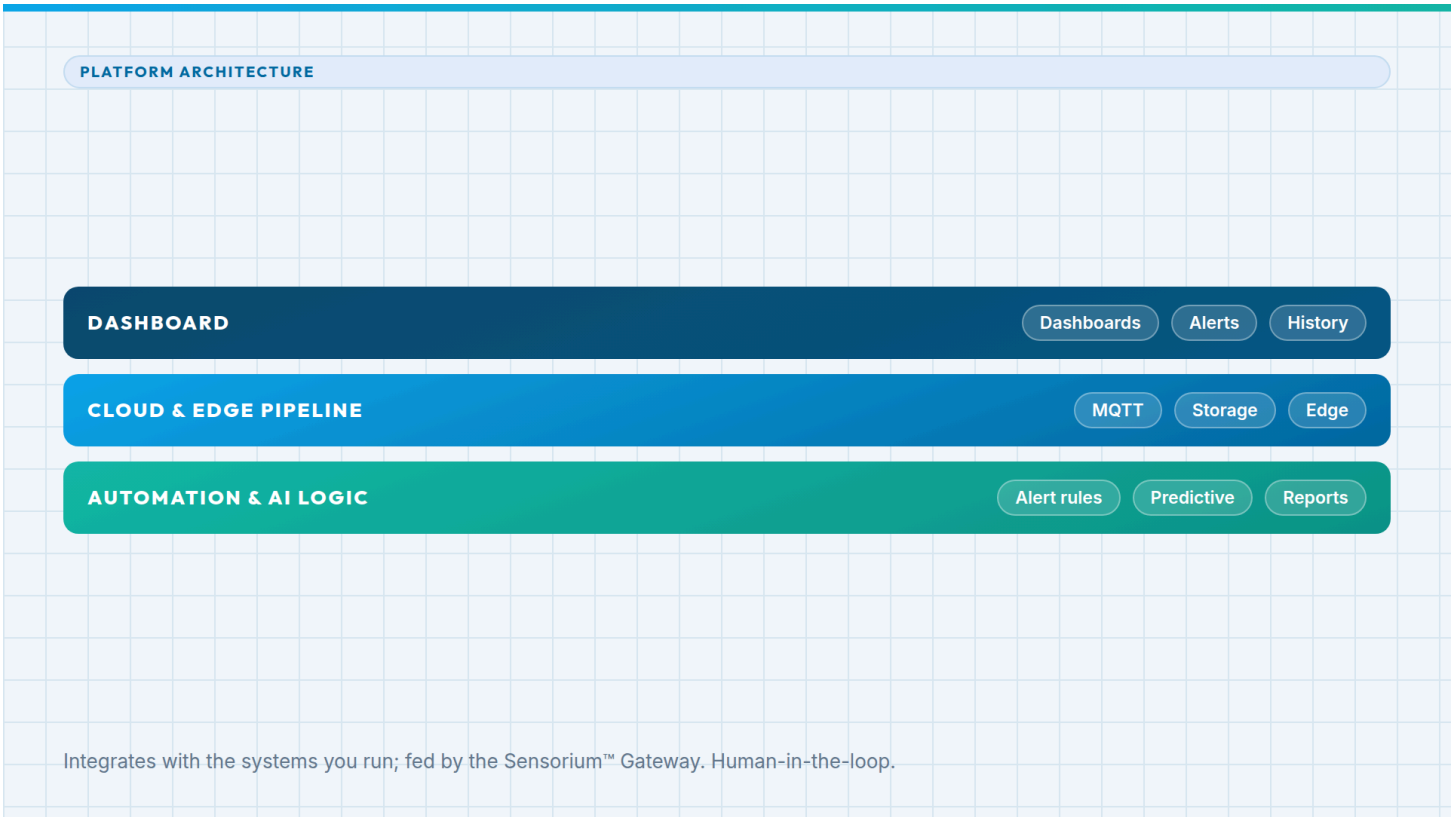

Figura FIG-002 — Las capas de Monitoreo, Automatización y Asistencia de IA, alimentadas por el Sensorium™ Gateway e integradas con SCADA y ERP.

CAPA	SUBTÍTULO	QUÉ HACE	DÓNDE EN ESTA GUÍA
Monitoreo	Paneles y alertas	Visualización de telemetría en tiempo real y generación de alertas	§5
Automatización	Flujos de trabajo e integraciones	Lógica basada en reglas: disparar acciones de ERP, sincronizar dispositivos, integrar entre sistemas	§6
Asistencia de IA	Asistentes con IA	Asistentes Triage, Compliance, Reporting y Summary — sugieren, señalan e informan; una persona decide	§7

Los cuatro asistentes con IA —**Triage**, **Compliance**, **Reporting** y **Summary**— residen dentro de la capa de Asistencia de IA y se presentan en §7. Son únicamente de apoyo a la decisión: ninguno de ellos toma acciones autónomas ni aplica políticas.

1.3 Dónde se sitúa la Plataforma en el ecosistema

El ecosistema 5Tech sigue una cadena **Sense** → **Connect** → **Decide**:

1. **Sense** — los dispositivos de campo Sensorium™ (Zone Awareness, SmartBolt) detectan condiciones en el campo.
2. **Connect** — el Sensorium™ Gateway agrega y preprocesa sus datos y los envía por enlace ascendente a través de MQTT.
3. **Decide** — la **5Tech Platform** (este producto) convierte esos datos en monitoreo, automatización y recomendaciones asistidas por IA sobre las que las personas actúan, que pueden fluir hacia SCADA/ERP y de vuelta a los dispositivos.

Las **Soluciones** empaquetadas —Gestión de flotas y Monitoreo de obras de construcción— se construyen sobre esta cadena y usan la Plataforma como su capa de software.

1.4 Conceptos y términos clave

TÉRMINO	SIGNIFICADO EN ESTA GUÍA
Sitio	Una ubicación física o agrupación de activos cuyos dispositivos reportan a la Plataforma.
Dispositivo	Una unidad de campo cuyos datos llegan a la Plataforma a través del Sensorium™ Gateway.
Telemetría	El flujo de mediciones que reporta un dispositivo (valores a lo largo del tiempo).
Evento	Un suceso discreto derivado de la telemetría (p. ej., el cruce de un umbral).
Alerta	Un evento presentado a los operadores para su atención, que lleva una gravedad.
Flujo de trabajo	Una regla de automatización: un disparador, condiciones opcionales y una o más acciones.
Integración	Una conexión entre la Plataforma y un sistema externo (SCADA, ERP).
Asistente con IA	Una función asistida por IA (Triage, Compliance, Reporting o Summary) que sugiere, señala o informa — una persona decide.
Política	Las reglas y umbrales configurables que rigen el comportamiento de un asistente.
Acción	La salida de un flujo de trabajo, o una persona que actúa sobre la sugerencia de un asistente (notificar, disparar una acción de ERP, sincronizar un dispositivo).
Registro de auditoría	El sistema de registro determinista y con detección de manipulaciones de la Plataforma (§8) — distinto del asistente de IA Reporting.

2. Acerca de esta guía

- **Público.** Operadores, supervisores y administradores que usan la 5Tech Platform. No se presupone programación; las tareas de administración presuponen el nivel de acceso adecuado (§4).
- **Alcance.** Uso cotidiano de Monitoreo, Automatización y Asistencia de IA, además del control de acceso, la auditabilidad, la administración, el mantenimiento, la seguridad, la resolución de problemas y el soporte. El despliegue, la puesta en marcha y la ingeniería de integración se entregan como servicios de 5Tech (§13.2) y quedan fuera del alcance aquí.
- **Convenciones.** Las listas numeradas son procedimientos — realice un paso a la vez, en orden. ‡ marca un valor propuesto, típico del sector, incluido para que la guía no contenga

espacios en blanco; no es definitivo ni contractual y se confirma en el despliegue. `[TBD]` marca un término legal/contractual que no debe inventarse. Las figuras se referencian como *Figura FIG-00N*.

- **Documentos relacionados.** Consulte §13.4.

---

3. Seguridad y límites de operación

Este es un **producto de software**: no tiene peligros físicos y no usa símbolos de peligro. Este breve capítulo establece los límites de operación que debe entender antes de confiar en la Plataforma. El acceso, los roles, la seguridad y el tratamiento de datos se tratan en §4, §8 y §11.

3.1 No es un sistema de protección con clasificación de seguridad

> **AVISO — Solo apoyo a la decisión, no un sistema de seguridad.** El monitoreo, las alertas y los asistentes con IA de la 5Tech Platform son **herramientas de apoyo a la decisión, no un sistema de protección con clasificación de seguridad**. **No** reemplazan la protección de las máquinas, los circuitos de parada de emergencia, los enclavamientos ni un sistema instrumentado de seguridad (SIS), y **no** deben ser el único medio de protección del personal o los equipos. Esto es coherente con los dispositivos de campo, que no son controladores de seguridad. La protección continua no depende de la Plataforma, de su ruta de red ni de su disponibilidad.

3.2 Principio de intervención humana

La Plataforma está diseñada para que sea una **persona quien decide**. Los asistentes con IA (§7) analizan datos para **sugerir, señalar e informar** — nunca toman acciones autónomas ni aplican políticas por sí mismos. Los flujos de trabajo de automatización (§6) ejecutan únicamente las reglas que una persona ha configurado y habilitado, y actúan sobre sistemas en vivo (incluidos SCADA/ERP), por lo que se prueban antes de confiar en ellos. Las alertas requieren un reconocimiento humano (§5.2); reconocer una alerta no elimina por sí mismo la condición subyacente.

---

4. Acceso, roles y permisos

El acceso a la Plataforma se rige por el **control de acceso basado en roles (RBAC)**: lo que puede ver y hacer depende del rol que le asigne su administrador y de los sitios a los que esté delimitado.

4.1 Inicio de sesión

1. Abra un navegador web compatible (navegadores compatibles y versiones mínimas: §11.5).
2. Vaya a la URL de la Plataforma de su organización (proporcionada por su administrador de 5Tech).
3. Inicie sesión con las credenciales de su organización. La autenticación se realiza mediante **inicio de sesión único (SSO vía SAML 2.0 / OIDC)‡** con **autenticación multifactor (MFA)‡** donde esté habilitada (§11.3).
4. Verifique que el **sitio** correcto esté seleccionado en la barra superior antes de comenzar.

Si el inicio de sesión falla, consulte §12 (Resolución de problemas) y §13 (Soporte).

4.2 Roles y permisos — la matriz RBAC

La Plataforma aplica el modelo de roles **definitivo** que se muestra a continuación. A cada cuenta se le asigna exactamente un rol y se delimita a uno o más sitios; el rol determina los permisos, y la delimitación determina a qué sitios se aplican esos permisos. Los administradores pueden delimitar cualquier rol a sitios específicos.

PERMISO	VISUALIZADOR	OPERADOR	SUPERVISOR	ADMINISTRADOR
Ver paneles y telemetría	✓	✓	✓	✓
Ver informes y resúmenes	✓	✓	✓	✓
Reconocer alertas	—	✓	✓	✓
Crear / editar / habilitar flujos de trabajo	—	✓	✓	✓
Configurar políticas de asistentes de IA (Triage · Compliance · Reporting · Summary)	—	—	✓	✓
Ver el registro de auditoría (§8)	—	—	✓	✓
Exportar datos (telemetría / informes / auditoría)	—	—	✓	✓
Gestionar integraciones (SCADA / ERP)	—	—	—	✓
Gestionar usuarios y roles	—	—	—	✓
Gestionar ajustes de seguridad, retención y despliegue	—	—	—	✓

> **AVISO.** Los cambios en los flujos de trabajo y en las políticas de los asistentes de IA afectan a las operaciones en vivo. Solo deben realizarlos las cuentas con el rol adecuado, los cambios deben revisarse antes de habilitarlos, y cada cambio queda registrado en el registro de auditoría (§8).

---

5. Monitoreo — paneles y alertas

La capa de Monitoreo proporciona **visualización de telemetría en tiempo real y generación de alertas**. El panel de monitoreo se muestra en la *Figura FIG-001* (la portada de esta guía).

5.1 Lectura del panel de monitoreo

El panel presenta el estado en vivo del sitio seleccionado —indicadores clave, gráficos de telemetría y un panel de alertas activas—. Las tarjetas, la disposición y las etiquetas exactas son preliminares.

Para abrir un panel

1. Inicie sesión y confirme que el sitio correcto está seleccionado (§4.1).
2. Abra el espacio de trabajo de **Monitoreo** desde la barra de navegación.
3. Seleccione el panel del sitio o activo que desea ver.
4. Confirme que los datos están en vivo — el indicador de actualidad / última actualización debe estar al día.

5.2 Trabajo con alertas

Las alertas presentan eventos que requieren atención, clasificados por **gravedad** (las gravedades más altas son más urgentes).

Para reconocer una alerta

1. En el espacio de trabajo de **Monitoreo**, abra el panel de **Alertas activas**.
2. Seleccione la alerta para ver su detalle (dispositivo de origen, hora, gravedad, telemetría relacionada).
3. Realice primero cualquier acción operativa necesaria; luego seleccione **Reconocer**.
4. Verifique que la alerta salga de la lista activa y quede registrada en el historial.

> **AVISO.** Reconocer una alerta registra que fue vista y atendida (y se escribe en el registro de auditoría, §8); no resuelve por sí mismo la condición subyacente. Confirme que la condición se ha despejado en la telemetría.

5.3 Relación con los asistentes con IA

El asistente **Triage** (§7.1) puede priorizar los eventos entrantes para que las alertas más críticas suban a la parte superior del panel de Alertas activas. Por lo tanto, lo que ve en Monitoreo está determinado por la política de Triage — si la priorización de alertas parece incorrecta, revise los ajustes de Triage con un administrador.

---

6. Automatización — flujos de trabajo e integraciones

La capa de Automatización es la **capa lógica**. Le permite disparar acciones de ERP, sincronizar dispositivos e integrar entre sistemas sin escribir código — mediante la creación de **flujos de trabajo**.

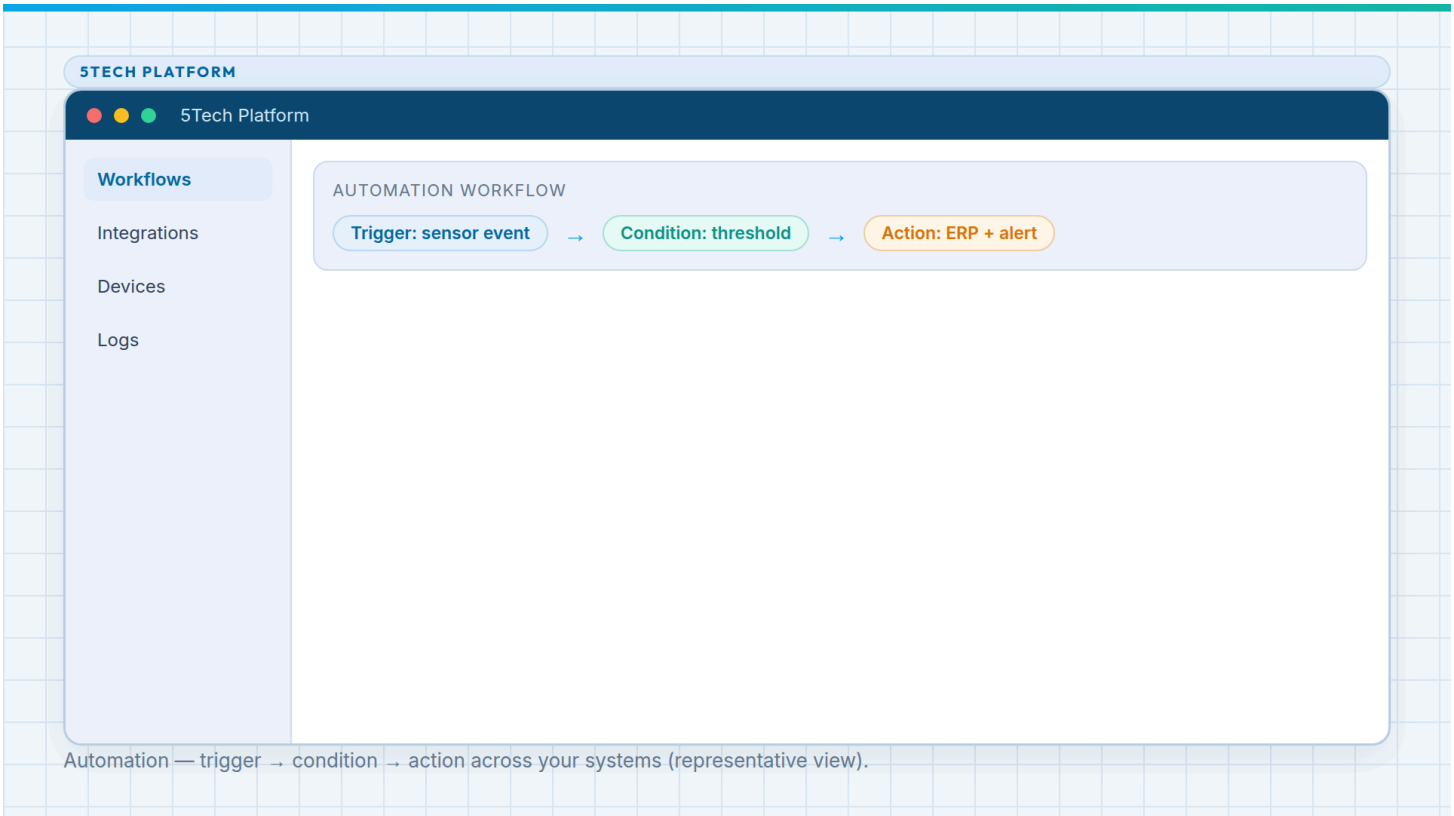

Figura FIG-005 — El constructor de flujos de trabajo de automatización: un disparador, condiciones y acciones conectados en una regla.

6.1 Anatomía de un flujo de trabajo

Un flujo de trabajo tiene tres partes:

- **Disparador** — lo que lo inicia (por ejemplo, una alerta o un evento de sensor).
- **Condición(es)** — pruebas opcionales que deben cumplirse para que el flujo de trabajo continúe.
- **Acción(es)** — lo que hace: notificar a un operador, disparar una acción de ERP, sincronizar un dispositivo o invocar otro sistema integrado.

La *Figura FIG-005* muestra estos elementos conectados en el lienzo del constructor.

6.2 Creación de un flujo de trabajo

Para crear un flujo de trabajo

1. Abra el espacio de trabajo de **Automatización** desde la barra de navegación (requiere rol de Operador o superior — consulte §4.2).
2. Cree un nuevo flujo de trabajo y asígnele un nombre claro y descriptivo.
3. Añada un bloque de **Disparador** y elija el evento que debe iniciar el flujo de trabajo.
4. Añada los bloques de **Condición** necesarios para delimitar cuándo se ejecuta el flujo de trabajo.
5. Añada uno o más bloques de **Acción** (notificar, acción de ERP, sincronización de dispositivo, invocación de integración).
6. Revise el flujo de trabajo conectado de principio a fin para verificar su corrección.
7. Guarde el flujo de trabajo. Permanece inactivo hasta que lo habilite en el paso siguiente.

Para habilitar un flujo de trabajo

1. Abra el flujo de trabajo guardado.
2. Confirme que el disparador, las condiciones y las acciones son correctos.
3. Conmute el flujo de trabajo a **Habilitado**.
4. Verifique que aparezca como activo y, cuando sea posible, pruébelo con un disparador controlado antes de confiar en él en producción.

> **AVISO.** Los flujos de trabajo habilitados actúan sobre sistemas en vivo, incluidas las acciones de SCADA/ERP. Pruebe de forma controlada antes de habilitar en producción, y cambie un flujo de trabajo a la vez. Los eventos de habilitación/deshabilitación y de edición quedan registrados en el registro de auditoría (§8).

6.3 Integraciones (SCADA y ERP)

La Plataforma se integra con los sistemas **SCADA** y **ERP** existentes para que los flujos de trabajo puedan leer contexto de —y enviar acciones a— los sistemas que ya opera. Establecer una integración (endpoints, credenciales, mapeo de campos) forma parte del despliegue y se entrega como un servicio de 5Tech (§13.2).

Una vez que existe una integración, refiérase a ella desde el bloque de **Acción** de un flujo de trabajo (§6.2) — por ejemplo, «crear una orden de trabajo de ERP» o «sincronizar un ajuste de dispositivo».

---

7. Asistencia de IA — configuración de los asistentes con IA

La capa de Asistencia de IA proporciona **asistentes con IA** que **analizan datos para sugerir, señalar e informar**. Funcionan **con intervención humana**: un asistente nunca toma acciones autónomas ni aplica políticas por sí mismo — una persona revisa su salida y decide. Hay cuatro asistentes disponibles.

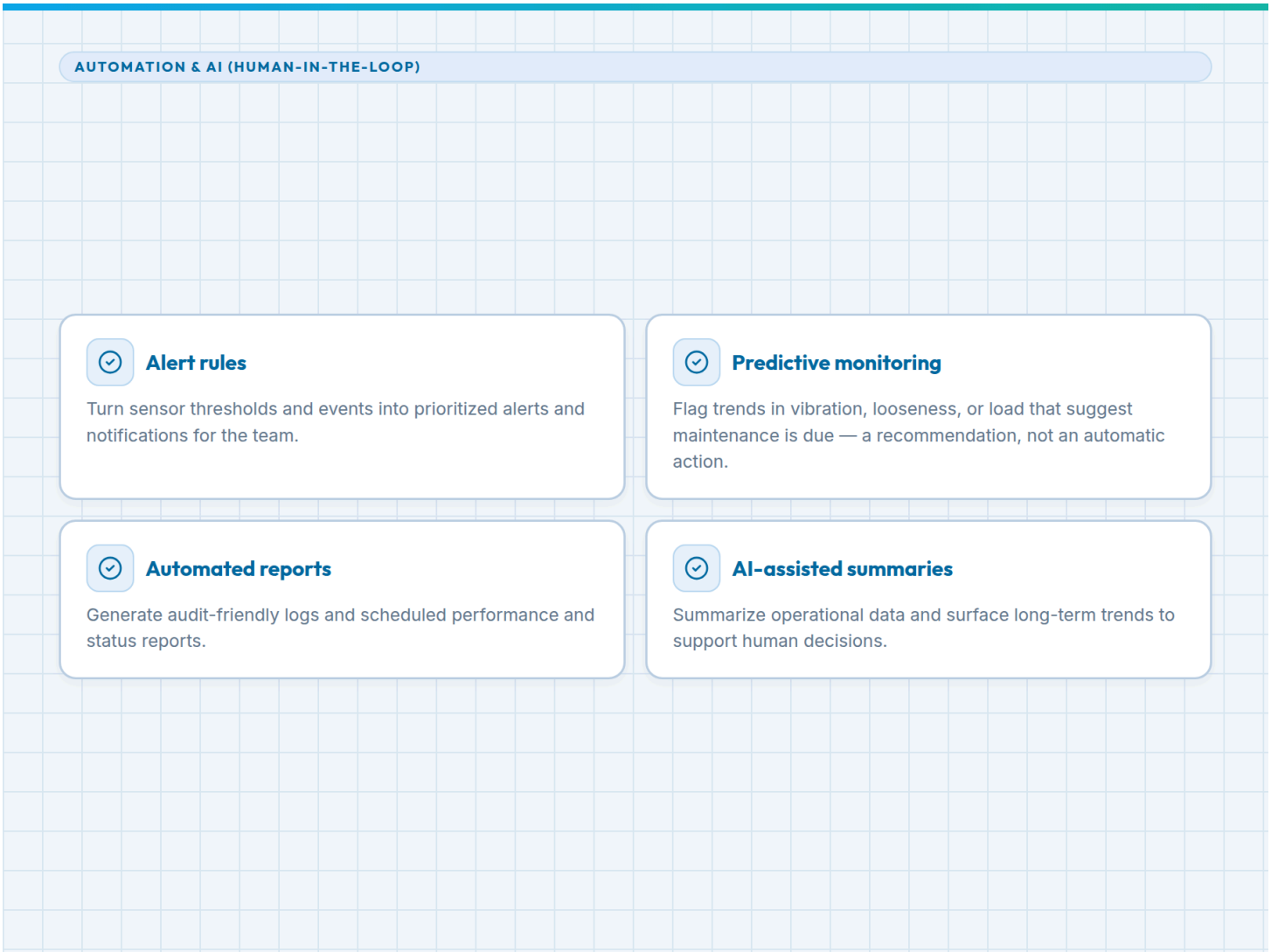

Figura FIG-003 — Los cuatro asistentes con IA —Triage, Compliance, Reporting y Summary— y lo que cada uno sugiere, señala o informa. Una persona decide.

ASISTENTE	QUÉ HACE
Triage	Prioriza y enruta los eventos críticos para la atención del operador
Compliance	Señala problemas de política, seguridad y umbrales/tendencias **solo para revisión humana**
Reporting	Produce informes legibles por personas e informes programados (no es el registro de auditoría — consulte §8)
Summary	Ofrece a los supervisores supervisión operativa y tendencias a largo plazo

Cada asistente se rige por una **política** — las reglas y umbrales que usted configura. Los asistentes solo sugieren, señalan e informan; las personas deciden y actúan. Configurar las políticas de los asistentes requiere rol de Supervisor o superior (§4.2), y cada cambio de política queda registrado en el registro de auditoría (§8).

7.1 Triage — priorización de eventos críticos

Triage ayuda a destacar qué eventos importan más, para que los operadores vean primero las alertas más críticas (§5.3). Sugiere una prioridad; los operadores siguen revisando y reconociendo cada alerta.

Para configurar Triage

1. Abra el espacio de trabajo de **Asistencia de IA** y seleccione **Triage** (requiere rol de Supervisor o superior, §4.2).
2. Revise las reglas y umbrales de priorización actuales.
3. Ajuste cómo se determinan la gravedad y la prioridad de los eventos para su sitio.
4. Guarde los ajustes; el cambio y su versión vigente quedan registrados en el registro de auditoría (§8).
5. Verifique el cambio en **Monitoreo** — confirme que las alertas se ordenan según lo previsto.

7.2 Compliance — señalamiento de problemas de política y seguridad para revisión

Compliance vigila la telemetría y la configuración frente a sus reglas de política, seguridad y umbrales, y **señala condiciones solo para revisión humana** — por ejemplo, una lectura que se aproxima a un umbral, o una condición de operación que se desvía de la política. **Señala y sugiere; no condiciona, detiene, bloquea ni aplica nada**, y no realiza ninguna determinación de cumplimiento — una persona revisa cada señalamiento y decide.

Para configurar Compliance

1. Abra el espacio de trabajo de **Asistencia de IA** y seleccione **Compliance** (rol de Supervisor o superior).
2. Revise las condiciones de política, seguridad y umbrales que vigila.
3. Actualice los umbrales y condiciones para que coincidan con sus requisitos de operación y política.
4. Guarde los ajustes; el cambio y su versión vigente quedan registrados en el registro de auditoría (§8).
5. Valide con un escenario controlado antes de confiar en sus señalamientos en producción.

> **AVISO.** Compliance solo genera señalamientos para revisión humana; no actúa por sí mismo y no certifica el cumplimiento. Revise los cambios con el responsable pertinente antes de habilitarlos en un sitio en vivo.

7.3 Reporting — informes breves e informes programados

Reporting produce los informes breves legibles por personas y los informes programados que facilitan la revisión de la actividad de la Plataforma — por ejemplo, un informe diario de operaciones o un informe de estado periódico.

> **AVISO.** Reporting es un asistente con IA que **genera resúmenes legibles a partir de datos**. **No** es el registro autoritativo de la Plataforma: el **registro de auditoría (§8)**, determinista y con detección de manipulaciones, es el sistema de registro, y existe independientemente de este asistente.

Para configurar Reporting

1. Abra el espacio de trabajo de **Asistencia de IA** y seleccione **Reporting** (rol de Supervisor o superior).
2. Elija qué informes breves/informes se producen y su programación (p. ej., diaria).
3. Establezca los destinatarios o destinos de los informes breves y de las exportaciones de informes.
4. Guarde. Confirme que se están produciendo los informes que necesita. El cambio de configuración queda registrado en el registro de auditoría (§8).

7.4 Summary — supervisión operativa y tendencias

Summary ofrece a los supervisores una vista de más alto nivel y en lenguaje llano de las operaciones y las tendencias a lo largo del tiempo.

Para usar Summary

1. Abra el espacio de trabajo de **Asistencia de IA** y seleccione **Summary**.
2. Elija el/los sitio(s) y el rango de tiempo para la vista general.
3. Revise las tendencias destacadas y los indicadores de supervisión operativa.
4. Siga cualquier tendencia preocupante hasta **Monitoreo** (§5) para ver la telemetría subyacente.

7.5 El bucle de evento a acción

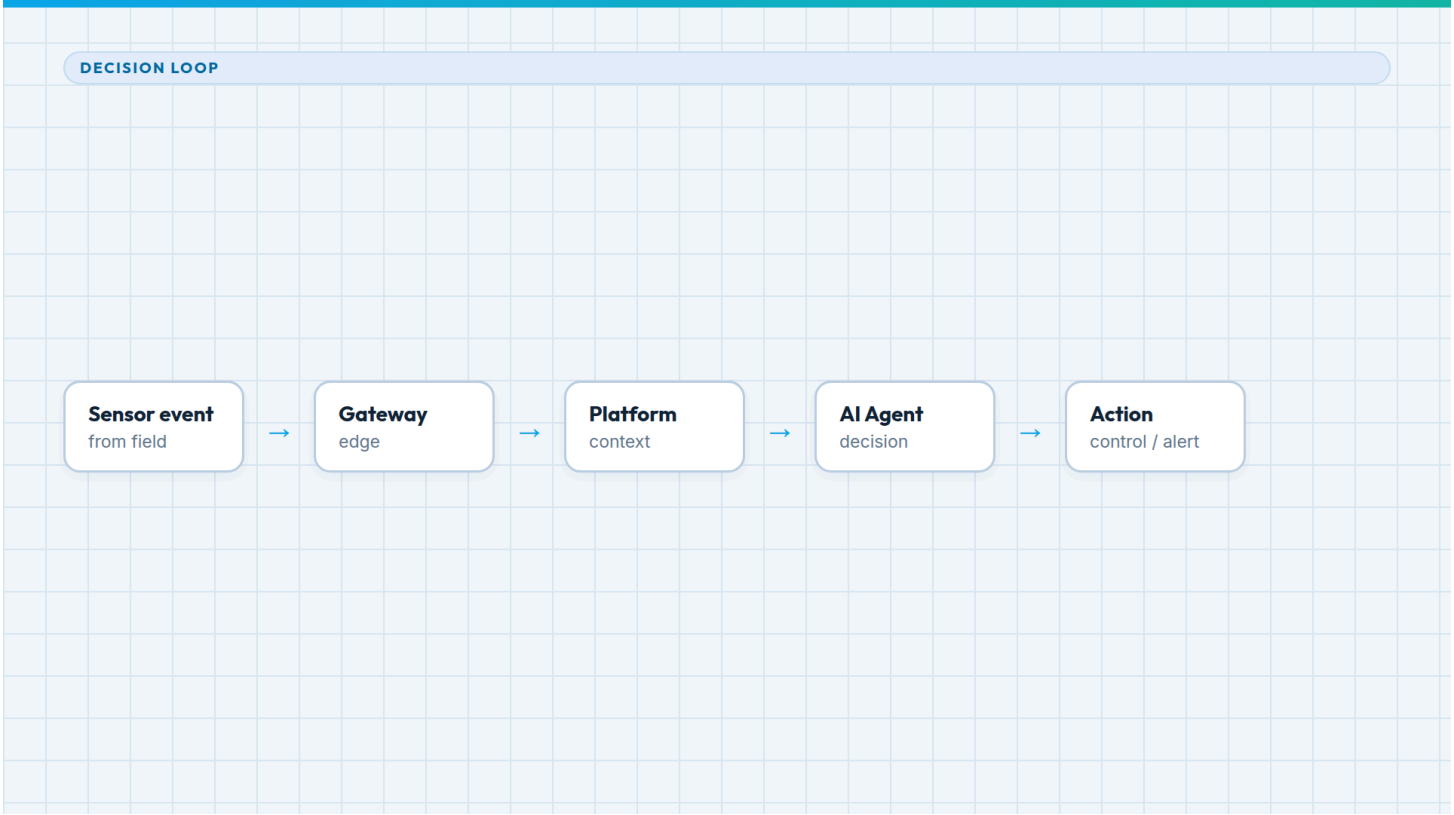

Figura FIG-004 — El bucle de evento a acción: un evento de sensor se prioriza y se coteja con la política mediante los asistentes, que presentan una sugerencia; una persona la revisa y decide la acción.

Los asistentes apoyan un bucle desde el campo hasta la acción que cierra una **persona**, como se muestra en la *Figura FIG-004*:

1. Un **evento de sensor** llega desde el campo a través del Sensorium™ Gateway.
2. Los **asistentes con IA** lo analizan — priorizándolo (Triage) y señalando cualquier preocupación de política o tendencia (Compliance) — y presentan una sugerencia a un operador.
3. Después de que una persona lo revisa y decide, resulta una **acción** — una alerta de operador, un flujo de trabajo de automatización (§6) o una acción de SCADA/ERP.
4. Los resultados retroalimentan como nueva telemetría; Reporting y Summary mantienen la actividad revisable, y el registro de auditoría (§8) la mantiene verificable.

---

8. Auditabilidad y sistema de registro

La auditabilidad es una **función central de la Plataforma**, provista por un **registro de auditoría determinista y con detección de manipulaciones** — el sistema de registro autoritativo de quién hizo qué y cuándo. Es **independiente del asistente de IA «Reporting» (§7.3)**: Reporting genera informes breves legibles por personas a partir de datos, mientras que

el registro de auditoría es un registro fijo y verificable por máquina que no depende de ninguna función de IA.

8.1 Qué es el registro de auditoría

- **Determinista y de solo anexado.** Las entradas se escriben una vez y nunca se editan; el registro no puede ser alterado ni eliminado por ningún usuario, **incluidos los administradores**.
- **Con detección de manipulaciones.** Las entradas están encadenadas criptográficamente (hash-chained‡) de modo que cualquier alteración de una entrada pasada es detectable, y cada entrada lleva una marca de tiempo UTC‡ sincronizada.
- **Independiente de los asistentes de IA.** Registra hechos, no interpretaciones de IA, y sigue operando con independencia de los asistentes Reporting, Summary, Triage o Compliance.

8.2 Qué se registra

El registro de auditoría registra, como mínimo:

- Inicios / cierres de sesión y eventos de autenticación (incluidos MFA e intentos fallidos).
- Cambios de rol y de permisos, y aprovisionamiento de usuarios / sitios.
- Creación / edición / habilitación / deshabilitación de flujos de trabajo (§6).
- Cambios de política de asistentes de IA con valores anteriores/posteriores y versión vigente (§7).
- Reconocimientos de alertas (§5.2).
- Adiciones, ediciones y eliminaciones de integraciones (§6.3).
- Exportaciones de datos y cambios de configuración/ajustes de seguridad (§11).

8.3 Uso del registro de auditoría

1. Abra el espacio de trabajo de **Administración** y seleccione **Registro de auditoría** (requiere rol de Supervisor o superior, §4.2).
2. Filtre por sitio, usuario, rango de tiempo o tipo de evento.
3. Revise las entradas; cada una es de solo lectura.
4. Exporte el registro filtrado para una auditoría en un formato abierto (CSV / JSON) donde tenga permiso de exportación (§4.2, §10.3).

El registro de auditoría se conserva durante **7 años‡** (o según su contrato) y está cubierto por los mismos controles de cifrado y residencia que el resto de sus datos (§11).

---

9. Administración

Las tareas de administración requieren el rol de Administrador (§4.2). Las pantallas y opciones exactas de administración son preliminares.

9.1 Usuarios y acceso

Para añadir un usuario

1. Abra el espacio de trabajo de **Administración** y vaya a la gestión de usuarios.
2. Añada al usuario con su nombre y su correo electrónico organizacional.
3. Asigne el rol adecuado (§4.2).
4. Delimite al usuario al/los sitio(s) correcto(s).
5. Guarde y confirme que el usuario recibe acceso según su configuración de SSO (§11.3).

Revise periódicamente a los usuarios y su acceso, y retire el acceso con prontitud cuando ya no sea necesario. Los cambios de usuario y de rol quedan registrados en el registro de auditoría (§8).

9.2 Sitios y dispositivos

Los sitios y sus dispositivos se aprovisionan como parte del despliegue. En el día a día, un administrador puede confirmar que los dispositivos de un sitio están reportando a través del Sensorium™ Gateway y que la telemetría está al día en **Monitoreo** (§5.1). La configuración de dispositivos reside en el Gateway y en los dispositivos de campo — consulte sus manuales (§13.4).

9.3 Integraciones

Gestione las integraciones de SCADA/ERP desde el espacio de trabajo de **Administración** (§6.3). Añadir, editar o eliminar una integración afecta a todos los flujos de trabajo que dependen de ella — cambie con cuidado y verifique después los flujos de trabajo dependientes. Los cambios de integración quedan registrados en el registro de auditoría (§8).

---

10. Mantenimiento

El mantenimiento de la Plataforma mantiene su despliegue recuperable, actualizado y portable. Para el servicio en la nube, 5Tech realiza la mayor parte de esto en su nombre; para los despliegues locales / en el borde (§11.4), las tareas se comparten con su equipo según el

runbook de despliegue. Los valores a continuación son ‡ propuestos y se confirman en el despliegue.

10.1 Copia de seguridad y restauración

- **Nube.** Los datos se respaldan automáticamente con **copias de seguridad diarias cifradas‡** y recuperación a un momento específico dentro de **15 min‡** (el objetivo de punto de recuperación, §13.3). Las copias de seguridad se conservan **30 días‡**. Las restauraciones se verifican periódicamente‡.
- **Local / en el borde.** Las copias de seguridad se ejecutan según el runbook de despliegue en el almacenamiento que usted controla; verifique las restauraciones según su propia programación.

Para solicitar una restauración (nube)

1. Contacte con el soporte de 5Tech (§13) con el sitio, los datos afectados y el momento objetivo.
2. Confirme el alcance de la restauración y el punto de recuperación esperado con el soporte.
3. Verifique los datos restaurados en **Monitoreo** (§5) y en el registro de auditoría (§8) una vez completada.

10.2 Actualizaciones de software y cadencia de parches

- **Nube.** Las actualizaciones las aplica 5Tech de forma continua **sin acción del usuario**. Las versiones de funcionalidades ocurren aproximadamente **mensualmente‡**; los parches de seguridad se aplican en un plazo de **30 días‡** desde la publicación del proveedor, y los parches **críticos** en un plazo de **7 días‡**. Las ventanas de mantenimiento que puedan afectar a la disponibilidad se anuncian con al menos **5 días hábiles‡** de antelación.
- **Local / en el borde.** Las versiones se entregan **trimestralmente‡** con parches de seguridad **críticos** fuera de banda, aplicados por 5Tech o por su equipo según el acuerdo de despliegue.

10.3 Exportación y portabilidad de datos

Sus datos son portables y no quedan bloqueados:

- Exporte la telemetría, las alertas, los informes y el registro de auditoría en **formatos abiertos (CSV / JSON)‡** a través de la interfaz de usuario y la API REST‡, donde tenga permiso de exportación (§4.2).
- Solicite una **exportación completa del inquilino** en cualquier momento; se provee en un plazo de **30 días‡** en formatos abiertos.
- Los periodos de retención y la residencia de los datos exportados y almacenados se tratan en §11.

11. Seguridad, datos y despliegue

La seguridad y el tratamiento de datos son fundamentales para una plataforma cuyo valor es la auditabilidad y la confianza. Los controles a continuación son **‡** propuestos y se confirman como parte del despliegue; el registro de auditoría (§8) registra los cambios en cualquiera de ellos.

11.1 Cifrado en tránsito

Todo el tráfico de red está cifrado con **TLS 1.2 / 1.3‡** — el tráfico de navegador/API hacia la Plataforma sobre HTTPS, y la ingesta de telemetría MQTT desde el Sensorium™ Gateway sobre MQTT sobre TLS. No se ofrece ningún transporte en texto plano.

11.2 Cifrado en reposo

Los datos almacenados —bases de datos, almacenamiento de objetos y copias de seguridad— están cifrados en reposo con **AES-256‡** usando claves gestionadas‡.

11.3 Autenticación y MFA

- **Inicio de sesión único (SSO)** vía **SAML 2.0 / OpenID Connect (OIDC)‡** contra su proveedor de identidad, de modo que las cuentas sigan el proceso de alta/baja de su organización.
- **Autenticación multifactor (MFA)‡** (autenticador / TOTP‡) aplicada donde esté habilitada.
- Las sesiones inactivas expiran tras **30 min‡**. Los eventos de autenticación quedan registrados en el registro de auditoría (§8).

11.4 Modelo de despliegue

- **Nube (predeterminado).** SaaS multiinquilino, alojado y mantenido por 5Tech.
- **Nube de inquilino único, local o dispositivo de borde opcionales‡** donde los datos deban permanecer en infraestructura que usted controla. La paridad de funcionalidades entre modelos se confirma en el despliegue‡.

11.5 Navegadores compatibles

Use un navegador de escritorio actual y compatible — la versión principal actual y la anterior de:

NAVEGADOR	VERSIÓN MÍNIMA‡
Google Chrome	≥ 114‡
Microsoft Edge	≥ 114‡
Mozilla Firefox	≥ 115 ESR‡
Apple Safari	≥ 16‡

JavaScript y las cookies deben estar habilitados; se recomienda un viewport mínimo de **1280 × 720‡**.

11.6 Retención y residencia de datos

- **Retención (‡ propuesta, configurable por despliegue).** Telemetría **13 meses‡** (rodante); alertas y eventos **24 meses‡**; el registro de auditoría **7 años‡** (o según contrato).
- **Residencia.** Los datos en la nube se alojan en su **región seleccionada (Canadá, UE o EE. UU.)‡**; los despliegues locales / en el borde (§11.4) mantienen todos los datos en infraestructura que usted controla.

---

12. Resolución de problemas

Pruebe primero los pasos a continuación. Si un problema persiste, contacte con el soporte (§13) con el nombre del sitio, la hora en que ocurrió y cualquier identificador de alerta o de flujo de trabajo.

SÍNTOMA	CAUSA POSIBLE	ACCIÓN
No se puede iniciar sesión	Credenciales incorrectas, acceso caducado, MFA o interrupción de SSO/IdP	Confirme las credenciales y MFA; verifique con su administrador que el acceso está activo y que SSO funciona; consulte §4.1, §11.3
El panel muestra datos obsoletos o ningún dato	La telemetría no llega a la Plataforma (Gateway/dispositivo/enlace ascendente)	Compruebe el indicador de actualidad; confirme que el Gateway está en línea (manual del Gateway, §13.4); contacte con el soporte si los datos no se reanudan
No apareció una alerta esperada	Triage, umbrales o evento no generado	Revise Triage (§7.1) y los umbrales de alerta con un administrador
Demasiadas alertas o mal clasificadas	Triage no ajustado para el sitio	Ajuste Triage (§7.1); valide en Monitoreo
El flujo de trabajo no se ejecutó	Flujo de trabajo deshabilitado, disparador no coincidente o condición falsa	Confirme que el flujo de trabajo está habilitado (§6.2); revise su disparador y condiciones
Falló la acción de ERP/SCADA	Integración no configurada o no disponible	Verifique la integración en Administración (§9.3); contacte con el soporte si sigue no disponible
Falta un menú o una acción	Rol insuficiente	Confirme su rol con un administrador (§4.2)

13. Soporte y niveles de servicio

5Tech — *Future Innovative Vision Engineering* — es una empresa de automatización e informática con sede en Vancouver, BC, Canadá.

- **Web:** https://5tech.ca
- **Correo:** info@5tech.ca
- **Sede:** Vancouver, BC, Canadá

13.1 Soporte y soporte de mantenimiento

Para ayuda continua, 5Tech ofrece **Soporte de Monitoreo y Mantenimiento** — un acuerdo de soporte para ayudarle a ajustar alertas, reglas y flujos de trabajo y mantener el despliegue en buen estado.

- **Horario de soporte‡:** 08:00–18:00 PT, de lunes a viernes (excepto festivos).
- **Objetivo de respuesta a incidentes críticos‡:** en un plazo de 4 horas hábiles; escalado fuera de horario según contrato‡.

13.2 Servicios de despliegue e incorporación

El despliegue, la integración y la capacitación se entregan como servicios, no cubiertos por esta guía:

- **Piloto y Prueba de Valor** — un piloto/MVP enfocado para demostrar valor.
- **Soporte de Despliegue e Integración** — ayuda para implantar e integrar la Plataforma: puesta en marcha, capacitación e integración de ERP/EAM/SCADA.
- **Soporte de Monitoreo y Mantenimiento** — soporte continuo para ajustar y mantener el despliegue (§13.1).

13.3 Niveles de servicio (SLA) y términos

ELEMENTO	OBJETIVO (‡ PROPUESTO)
Disponibilidad / tiempo de actividad (nube)	**99.5 %‡** mensual, excluyendo el mantenimiento anunciado
Objetivo de punto de recuperación (RPO)	**≤ 15 min‡** (nube); local según runbook
Objetivo de tiempo de recuperación (RTO)	**≤ 4 h‡** (nube); local según runbook
Horario de soporte	08:00–18:00 PT, lun–vie‡ (§13.1)
Términos de garantía / licencia	`[TBD]` — legal/contractual, provisto en el acuerdo de suscripción; no se indica aquí porque no debe inventarse

Las cifras del SLA son objetivos **‡** propuestos y se confirman en su acuerdo de suscripción; los objetivos locales dependen del entorno controlado por el cliente.

13.4 Documentos relacionados

- **Hoja de datos del Gateway:** `datasheets/sensorium-gateway-datasheet/` — la capa Connect que alimenta la Plataforma.

- **Manual del Gateway:** `manuals/sensorium-gateway-manual/` — operación y configuración del Gateway.
- **Dispositivos de campo:** hojas de datos de Sensorium™ Zone Awareness y Sensorium™ SmartBolt — la capa Sense.
- **Soluciones:** Gestión de flotas y Monitoreo de obras de construcción — resultados construidos sobre esta cadena.

Al contactar con el soporte, tenga a mano: el nombre del sitio, la hora del problema, los usuarios o roles afectados, cualquier identificador de alerta/flujo de trabajo y (para administradores) las entradas pertinentes del registro de auditoría (§8).

Figuras

ID	TÍTULO	ARCHIVO	RELACIÓN DE ASPECTO	PROPÓSITO
FIG-001	Panel de monitoreo	`images/dashboard_monitoring.png`	16:9	Portada / imagen principal — el espacio de trabajo de monitoreo
FIG-002	Arquitectura de la Plataforma	`diagrams/platform_architecture.png`	16:9	Las tres capas + integración SCADA/ERP
FIG-003	Panorama de Automatización e IA	`diagrams/ai_agents_overview.png`	4:3	Los cuatro asistentes con IA (Triage · Compliance · Reporting · Summary) y lo que cada uno sugiere, señala o informa
FIG-004	Bucle de decisión	`diagrams/decision_loop.png`	16:9	Evento de sensor → sugerencia del asistente → una persona decide → acción
FIG-005	Constructor de flujos de trabajo de automatización	`images/automation_workflow_builder.png`	16:9	La vista del flujo de trabajo de automatización (maqueta de UI)

Esta guía es preliminar y está sujeta a cambios. Los valores marcados con ‡ son propuestos y se confirman en el despliegue; un `[TBD]` restante es un término legal/contractual. Consulte `revision.md` para el control de cambios y `references.md` para las fuentes. Destino de publicación web: `/resources/manuals/platform/`.